HQbird User Guide: (version 2020)

About this Guide

HQbird User Guide contains detailed description of functions and features of HQbird — advanced Firebird distribution, including with configuration examples and best practices recommendations.
# Table of Contents

Preface ................................................................................................................................. 8

1. Overview of HQbird ........................................................................................................... 9
   1.1. What is HQbird ........................................................................................................... 9
   1.2. What's new in HQbird 2020 ................................................................................... 9
   1.3. Feature matrix .......................................................................................................... 10

2. Installation of HQbird ....................................................................................................... 13
   2.1. Installing HQbird Server on Windows ................................................................. 13
   2.2. Installing HQbird Server for Windows using the installer ................................... 14
   2.3. Installing HQbird Administrator on Windows .................................................... 27
   2.4. Installing HQbird Server on Linux ...................................................................... 31
   2.5. Upgrade existing HQbird version ....................................................................... 33
   2.6. Registration of HQbird ......................................................................................... 35
   2.7. How to install community version of Firebird on Windows ................................ 29

3. Configuration of HQbird .................................................................................................. 40
   3.1. Initial configuration of HQbird FBDataGuard (backups, monitoring, alerts, etc) ... 40
   3.2. Monitoring and maintenance configuration in FBDataGuard ......................... 50

Overview of web-console .................................................................................................... 50

Parts of web-console .......................................................................................................... 50

Jobs ..................................................................................................................................... 50

Jobs widgets ........................................................................................................................ 50

Status types ......................................................................................................................... 51

Server: Active server ......................................................................................................... 52

Server: Auto updates ......................................................................................................... 53

Server: Agent Output Folder ......................................................................................... 54

Server: Replication Log ................................................................................................. 55

Server: Server log ............................................................................................................. 56

Server: Temp files ............................................................................................................. 57

Server: Firebird server folder .......................................................................................... 58

Database: General configuration ..................................................................................... 60

Database: Transactions ..................................................................................................... 60

Database: Lockprint .......................................................................................................... 61

Database: Index statistics recalculation .......................................................................... 65
Step 1: Configure HQbird for replication at the master ............................................. 167
   Asynchronous replication at master ................................................................. 168
How to copy replication segments from master server to the replica server? ........ 171
   Network share .............................................................................................. 171
   Cloud Backup/Cloud Backup Receiver ........................................................... 171
Step 2: Create a copy of master database ............................................................. 172
Step 3: Setup database for async replication at the replica(server) server ............ 173
6.4. Automatic initialization and re-initialization of replica .................................. 174
   How re-initialization works ............................................................................. 175
Troubleshooting asynchronous replication ......................................................... 175
6.5. Synchronous replication for Firebird ............................................................... 177
   Steps to setup synchronous replication .......................................................... 178
   Synchronous replication at master and replica ................................................. 179
   Replication parameters for testing synchronous replication ......................... 179
6.6. How to manually create replica of the database? .......................................... 181
   Creating copy online (with nbackup) .............................................................. 181
   What is {DATABASEGUID}? ........................................................................... 182
   How to set replica database to the master mode ............................................. 183
6.7. How to distinguish master database from replica .......................................... 184
   Using gstat -h .............................................................................................. 184
   With SQL query to the context variable SYSTEM.REPLICA ....................... 184
6.8. Optional parameters for replication ................................................................. 185
7. Performance enhancements .................................................................................. 187
   7.1. Pool of external connections ..................................................................... 187
   7.2. Cached prepared statements ...................................................................... 188
   7.3. TempSpaceLogThreshold: monitoring of big sorting queries and BLOBs .... 189
   7.4. SortDataStorageThreshold: REFETCH instead SORT for wide record sets ... 190
   7.5. Multi-thread sweep, backup, restore ......................................................... 191
7.6. Optional parameters for async replication ..................................................... 194
8. Encryption support .............................................................................................. 194
   8.1. OpenSSL files ........................................................................................... 194
How to encrypt and decrypt Firebird database .................................................... 194
   Demo package with client applications examples .......................................... 194
   Stage 1 — Initial encryption of the database ..................................................... 194
      1. Create the following alias in databases.conf ......................................... 195
      2. Check that the following files to server/plugins from the folder
         WinSrv64Bit_ServerPart\plugins ............................................................... 195
      3. Put the following files into Firebird root from the folder
         WinSrv64Bit_ServerPart ........................................................................... 195
      4. Connect to the unencrypted database with isql and encrypt the database: ................................................................. 195
   Stage 2 — Connect to the encrypted database with the client application .... 197
   Step 3: backup and restore of the encrypted database ................................... 199
      Backup encrypted Firebird database .......................................................... 200
      Restore the backup to the encrypted Firebird database ......................... 200
9. Authentication plugin for Execute Statement On External ................................. 202
   9.1. Installation of authentication plugin for ESOE ........................................... 202
   Authentication plugin files ............................................................................ 202
   Configuration ................................................................................................. 203
      In firebird.conf ......................................................................................... 203
      Keyfile ....................................................................................................... 203
      Mapping ..................................................................................................... 204
      Global mappings ....................................................................................... 205
Preface

1. About this Guide

HQbird User Guide contains detailed description of functions and features of HQbird – advanced Firebird distribution, including configuration examples and best practices recommendations.

2. About IBSurgeon

IBSurgeon (https://www.ib-aid.com) was founded in 2002 with the idea to provide InterBase and Firebird developers and administrators with services and tools focused on databases safety, performance and availability. In Russia, IBSurgeon is mostly known as iBase.ru, famous by its Russian InterBase and Firebird portal www.ibase.ru. IBSurgeon is a member of Firebird Foundation and, as a member of Technical Task Group, has strong relationship with Firebird Project, with direct representatives in Firebird-Admins and in Firebird Foundation Committee. Today, IBSurgeon serves thousands of companies worldwide with emergency, optimization and maintenance tools and various services. Our clients are medical institutions, financial organizations and ISVs in Germany, Brazil, Russia and other countries, and all who have applications based on Firebird and/or InterBase. The flagship project of IBSurgeon is HQbird, the advanced distribution of FirebirdSQL for big databases with enterprise features.
Chapter 1

Overview of HQbird

1.1. What is HQbird

HQbird is an advanced distribution of Firebird for enterprises, with the following list of features:

- Native one-to-many replication (2.5, 3.0)
  - Replicates databases with 1500+ connections
  - Asynchronous replication with 10 seconds delay
  - Synchronous replication
  - No triggers or other changes in schema required, DDL support, online re-initialization

- multi-thread backup, restore, and sweep;

- support for encryption;

- pool of execute on external connections;

- cached prepared statements;

- optimized configurations;

- backups automation, including cloud backups;

- database health monitoring;

- automatic performance and transactions reports;

- advanced transactions and queries monitoring (Trace, MON$ and FBScanner);

- database structure analysis;

- recovery toolset and database development GUI.

Also HQbird includes a performance self-test to measure Firebird performance on the specific hardware and OS configuration.

HQBird contains 2 parts: Server and Admin. The Server part has versions for Windows and Linux, and the administration part works on Windows only.

There are 3 editions of HQbird: Standard, Professional and Enterprise.

1.2. What's new in HQbird 2020

HQbird 2020 is the biggest release since the replication support in HQbird 2016, it contains a lot of new features:
• Multi-thread Sweep, Backup, Restore in Firebird 2.5 and 3.0
  • Sweep – up to 6x faster
  • Backup – up to 5x faster
  • Restore – up to 2x faster

• Speed-up heavy reports (up to 5x times) (Firebird 3.0)
  • Queries with many fields SELECT with GROUP BY, ORDER BY, etc can use REFETCH plan to gain up to 5x performance
  • New parameter in firebird.conf to manage sort behavior
  • No changes in applications sources/SQLs required

• Enhanced performance monitoring reports (2.5, 3.0)
  • Low performance impact, easy to schedule
  • Top queries reports: time-consuming, frequent, CPU-consuming, disk, etc

• Encryption Plugin (3.0)
  • AES256 strong encryption, for Windows and Linux
  • gbak with encryption support, decrypt low-level tool (for recovery)
  • Examples of sources for Delphi, NET, PHP, Java
  • Support of encrypted databases in HQbird

• Authentication plugin for transparent Execute Statement On External (3.0)
  • allows establish trusted authentication of ESOE without password

• RSA-UDR: sign documents (strings and BLOBs) (3.0)
  • Public/Private Keys generation
  • Functions to calculate digest, sign, verify signature

• Enhanced silent installation and registration – on Windows

• Automatic upgrades of HQbird: checking and download, 1 click install

• Control Center For Firebird (2.5, 3.0, for subscription customers only)
  • Review status of many Firebird servers on the same page
  • Notifications about successful backups and critical problems

1.3. Feature matrix

Below there is the feature matrix for HQbird editions.

<table>
<thead>
<tr>
<th>Features</th>
<th>Standard</th>
<th>Professional</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimized configurations</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Backups</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Automatic Performance Reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SQL queries tracking</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Transactions tracking</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Overview of HQbird

<table>
<thead>
<tr>
<th>Features</th>
<th>Editions</th>
<th>Standard</th>
<th>Professional</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database structure analysis</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Performance self-test suite</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL development, design&amp;debugging</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication and high availability</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool of Execute On External statements</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cached prepared statements</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-thread backup, sweep, restore</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption support</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced authentication and security features</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It is possible to single out components in the HQbird modules that are responsible for certain operations (such as backup, monitoring, database repair).

The table below shows how features are distributed among the HQbird modules:

<table>
<thead>
<tr>
<th>Features</th>
<th>Modules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup (automated verified and incremental backup)</td>
<td>FBDataGuard</td>
<td>FBDataGuard runs on the server side and performs all kinds of backup</td>
</tr>
<tr>
<td>Optimized Configurations (balanced, read-intensive and write-intensive)</td>
<td>FBDataGuard, a collection of optimized configurations</td>
<td>The optimized configuration file can be customized on the basis of recommendations from FBDataGuard</td>
</tr>
<tr>
<td>Performance Test Suite (hardware score)</td>
<td>Performance Test Suite</td>
<td>The test measures the hardware performance</td>
</tr>
<tr>
<td>Monitoring SQL Queries (MON $, TraceAPI and FBScanner)</td>
<td>Performance Monitor, MON $Logger, FBScanner</td>
<td>Three different monitoring methods are used in different scenarios</td>
</tr>
<tr>
<td>Health Monitoring (online validation, database health check, log analysis)</td>
<td>FBDataGuard</td>
<td>Everything is carried out on the server. FBDataGuard sends notifications by e-mail.</td>
</tr>
<tr>
<td>Transaction Tracking (dynamic analysis of transaction markers)</td>
<td>FBDataGuard, Transaction Monitor, MON $Logger</td>
<td>FBDataGuard tracks problems with transactions, Transaction Monitor and MON$Logger show the dynamics of changes and the current status of active transactions.</td>
</tr>
</tbody>
</table>
## Overview of HQbird

<table>
<thead>
<tr>
<th>Features</th>
<th>Modules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Structure Analysis</strong> (table and index sizes, fragmentation, versioning, etc.)</td>
<td>Database Analyst</td>
<td>Database Analyst analyses the database structure in detail and shows warnings and recommendations.</td>
</tr>
<tr>
<td><strong>SQL Development &amp; Debugging</strong> (a GUI tool for developing databases and queries)</td>
<td>SQL Studio</td>
<td>SQL Studio is a powerful tool for developing and debugging database objects and SQL queries.</td>
</tr>
<tr>
<td><strong>Recovery</strong> (database recovery, backup recovery, record undeleting)</td>
<td>FirstAID, FBDataGuard, IBBackupSurgeon, IBUndelete</td>
<td>FirstAID repairs databases when they get corrupted, FBDataGuard stores important metadata thus increasing the chances of successful repairs, IBBackupSurgeon exports data from corrupted backup copies. IBUndelete can undo records deletion.</td>
</tr>
<tr>
<td><strong>High Availability</strong> (replication)</td>
<td>The HQbird Enterprise edition includes replication and high availability tools.</td>
<td></td>
</tr>
<tr>
<td><strong>Performance improvements</strong> (pool of Execute On External and Cached prepared)</td>
<td>HQbird Enterprise</td>
<td>HQbird Enterprise includes performance improvements.</td>
</tr>
<tr>
<td><strong>Multi-thread backup, sweep, restore</strong></td>
<td>HQbird Enterprise</td>
<td></td>
</tr>
<tr>
<td><strong>Encryption support</strong></td>
<td>HQbird Enterprise</td>
<td></td>
</tr>
<tr>
<td><strong>Enhanced authentication and security features</strong></td>
<td>HQbird Enterprise</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 2

Installation of HQbird

HQbird contains 2 parts: Server and Admin. Let's consider how to install them.

2.1. Installing HQbird Server on Windows

HQbird Server 2020 includes Firebird 2.5 and 3.0 with replication, multi-thread support and other enhancements as part of its installer, so Firebird must be installed as part of HQbird. It is mandatory to install Firebird bundled with HQbird Server installer, if you plan to use replication (it also requires HQbird Enterprise license, full or trial) and other enhancements.

Optionally you can choose HQbird Standard, which will not install Firebird, so you can use previously installed Firebird – in this case, make sure that installed version is compatible (2.5.2, 2.5.5, 2.5.6, 2.5.7, 2.5.8, 2.5.9, 3.0.x).

Please note, that only Firebird 2.5 and 3.0 are fully supported in HQbird, the old Firebird versions are supported partially. We offer the comprehensive Firebird migration service with guaranteed and fast result to migrate Firebird to the latest version.

Silent installation on Windows

The fastest way to install HQbird is to use the silent installation command.

In the example below we will install HQbird Enterprise with Firebird 3.0 into c:\HQbird, configuration will be c:\HQbirdData\config, output in c:\HQbirdData\output.

HQBirdServer2020.exe /VERYSILENT /SP= /TYPE="hqbird30x64" /DIR="C:\HQbird2020" /CONFIGDIR=C:\HQBirdData\config /OUTPUTDIR=C:\HQBirdData\output

The following parameters are mandatory to perform the silent installation:

- /VERYSILENT /SP - options to perform the silent installation

- /TYPE – what HQbird version should be installed. If you are doing silent upgrade, make sure the version is the same as it was installed previously.
  - "HQBird25x86" - "HQbird Enterprise (with Firebird 2.5 x32)";
  - "HQBird25x64" - "HQbird Enterprise (with Firebird 2.5 x64)";
  - "HQBird30x86" - "HQbird Enterprise (with Firebird 3.0 x32)";
  - "HQBird30x64" - "HQbird Enterprise (with Firebird 3.0 x64)";
  - "StdHQBird" - "HQbird Standard (no Firebird engine)".

- /DIR - where to install HQBird. If you are doing silent upgrade, make sure the version is the same as it was installed previously.
Installation of HQbird

- /CONFIGDIR – where to store configuration data for HQbird.
- /OUTPUTDIR – where to store output data (default location for backups, performance reports, etc).

Optional parameters for the silent installation of HQbird:

- /DGPORT=8082 – port for web interface of HQbird (FBDataGuard)
- /fbport=3050 - port for Firebird to be installed with HQbird Enterprise
- /LOG=C:\temp\log.txt - where to store installation log
- /REGEEMAIL=youremail@company.com - email to perform the automatic registration of HQBird
- /REGPASS=yourpassword – password from IBSurgeon Deploy Center account to register HQbird
- /REGTYPE=S|E|T == Standard, Enterprise, Trial – license type, must be specified if you need to register HQbird during the installation
- /EAHOST=smtp.company.com – SMTP server for email alerts
- /EAPORT=25 – SMTP port for email alerts
- /EALOGIN=support – SMTP login to send email alerts
- /EAPASSWORD=psw – SMTP password to send email alerts
- /eato=support@email.to – where to send email alerts
- /eafrom=someemaildg@company.com – from address
- /EAENABLED=true – enable or disable email alerts
- /EADEFALT=true – send a copy of email alerts to IBSurgeon Control Center

Please note, that in a case of error, for example, if you are trying to run silent installation to install HQbird to the location which is different from the current location, the error message window will popup and installation will be canceled.

2.2. Installing HQbird Server for Windows using the installer

Download HQbird from https://ib-aid.com/en/download-hqbird

The distribution package of HQbird server is the same for the 32-bit and 64-bit versions of the Firebird engine.
Make sure that HQbird installer is signed with valid IBSurgeon certificate («iBase LLC») and run it:

![Installer signature](image1.png)

Figure 2.1. Installer is signed with IBSurgeon digital signature: iBase LLC

![Confirmation to start installation](image2.png)

Figure 2.2. Confirmation to start the installation process

The HQbird Server Side installation wizard will be launched after that and it will take you through several steps, such as agreeing to the license agreement and selecting the installation folder.
At first, the installer will ask you where to install HQbird:

![Figure 2.3. Where to install HQbird](image)

We recommend to use the default location \texttt{c:\HQbird}, but you can use any suitable location.
After that, you should select folders for storing configuration files, backup copies of databases, statistics and HQbird log files:

![Select locations dialog]

**Figure 2.4. Select folders for HQbird configuration and log files**

By default, the installation wizard offers to create folders for configuration and log files in `C:\HQbirdData`.

**Note**

Usually, we recommend selecting a disk with a large amount of free space for this purpose, but you can configure it later.

If configuration files already exist in the selected location, the installation wizard will display the corresponding warning:

![Warning dialog]

**Figure 2.5. Warning about existing configuration files**
We recommend the automatic upgrade, so default answer should be Yes.

However, you can choose to create fresh configuration of HQbird, and click No – it this case the installer will warn you that existing configuration files will be moved:

![Figure 2.6. Confirmation of backup](image)

**Figure 2.6. Confirmation of backup**

In case of choosing Cancel, you need to specify the different location for the configuration and output/backup files.

After you confirm it, the folder with the existing configuration files will be renamed and the installation will continue.
After that, you will see the installation step where you can select components to be installed:

![Select Components](image)

**Figure 2.7. Select components from HQbird Server Side to be installed**

We recommend that you install HQbird Enterprise, which contains all HQbird components and Firebird, to avoid further configuration. All HQbird modules are installed in the inactive mode and do not affect the operation of the Firebird server until they are configured or used.

If you select to install HQbird Enterprise (i.e., with Firebird), it will install Firebird in the subfolder of HQbird installation, by default `C:\HQBird\Firebird25` or `C:\HQBird\Firebird30`. 
Installation of HQbird

Then, you will be asked to specify the port for HQbird FBDataGuard (web interface to manage HQbird):

![Specify port for HQbird FBDataGuard](image)

**Figure 2.8. Specify port for HQbird FBDataGuard – management tool with web interface**

We recommend to keep 8082, but sometimes this port can be occupied, so you can change it.
Installation of HQbird

After that, the installer will ask about email settings to be used to send email alerts:

![Email alerts settings screenshot](image.png)

**Figure 2.9. Email alerts settings**

**Note**

You can skip this step: all email alerts can be set later in web interface.
Then, the installation wizard will ask to specify the port for Firebird engine installed with HQbird:

![Setup - HQBird Server Side 2020](image)

**Figure 2.10. Specify port for Firebird server**

By default, the port is 3050. If the port will be occupied by another running Firebird, the installation wizard will warn you and make you choose another port. Or, you can stop and uninstall another Firebird service.

The checkbox “Add MaxParallelWorkers parameter to enable multi-threaded features” enables multi-threading support for backup, restore and sweep. You can learn more in the “Performance enhancements” chapter of the *Multi-thread sweep, backup, restore* section.
Then, only if you are installing HQbird Standard (i.e., without bundled Firebird), the installation wizard will ask you to specify the folder where Firebird is installed:

![Image of the installation wizard selecting the Firebird root folder]

**Figure 2.11. Confirm the location of the current Firebird instance (for HQbird Standard).**

**Attention!** During this step, the installation wizard checks the availability and compatibility of the installed Firebird version with HQbird. If the specified folder does not contain a correctly installed Firebird version, you will see the following warning:

![Image of the installation wizard warning]

**Figure 2.12. This warning from the installation wizard prompts you to select the correct Firebird folder.**

You should use Firebird version 2.5.5 or higher for HQbird Standard to be installed (see [How to Update Firebird for Windows](#)), or choose HQbird Enterprise to install the newest Firebird.
Then, you can specify the folder name and location in Windows menu:

![Screenshot of HQbird installation](image)

**Figure 2.13.** Choose Windows Start menu folder.
At the next step the installer will offer you to pre-configure HQbird to be used as master or replica server:

![Select Additional Tasks](image)

**Figure 2.14. Pre-configuration for replication.**

You can skip this step, this configuration can be done later.
The final step is a summary of components to be installed and their paths:

![Setup - HQBird Server Side 2020](image)

- **Setup type:** HQbird Enterprise (with Firebird 3.0 x64)
- **Destination location:** C:\HQbird
- **Destination directory for HQbird configuration files:** C:\HQBirdData\config
- **Destination location for HQbird output:** C:\HQBirdData\output
- **Selected components:**
  - HQbird Server Side
  - Firebird engine
    - 3.0 64-bit
  - HQbird FBDataGuard for Windows
  - Firebird configuration files
  - Replication plugins
  - Transaction monitor
  - OLTP Benchmark
  - Client libraries
- **Start Menu folder:** IBSurgeon\HQBird Server Side 2020

![Click Install to complete the installation.](image)

**Figure 2.15. Click Install to complete the installation.**

After that you have to activate HQbird (see How to Activate HQbird) and proceed to configure the HQbird components.
Installation of HQbird

At the end of installation process, you will be asked about next steps:

![Setup - HQBird Server Side 2020](image)

Figure 2.16. Post-installation steps.

### 2.3. Installing HQbird Administrator on Windows


The name of HQbird Administrator package is **HQbirdAdminNNNN.exe** (it is in the zip archive).
Run the installation wizard and follow the standard installation steps: digital signature check, license, then select the installation folder:

![Figure 2.17. Select where to install HQbird Admin.](image)

Figure 2.17. Select where to install HQbird Admin.
Select tools to install after that. We recommend that you install all tools.

![Select Components](image)

Figure 2.18. Select tools to install.

Follow the instructions after that. After the installation is over, you will be offered to launch the activation wizard. If you are installing HQbird Admin on the same computer where HQbird Server was already installed, the license will be automatically detected by HQbird Admin tools.

**How to install community version of Firebird on Windows**

The easiest way is to install Firebird bundled with HQbird – just choose the desired version during the installation. However, sometimes it is necessary to use HQbird with a community version of Firebird.

**Note**

Please note – to enable replication and performance features in HQbird Enterprise you need to install Firebird bundled with HQbird ServerSide.

To install Firebird separately, download the Firebird zip archive from [www.firebirdsql.org](http://www.firebirdsql.org)

Unpack the archive file to a suitable location (for instance, C:\Firebird25), after that copy the optimized configuration file `firebird.conf` (see Optimized Configurations below) to this folder.
Then, go to the Bin folder and then use the **Run As Administrator** option to run the batch file with the architecture you need.

- For Firebird 2.5 – run *install-superclassic.bat*.
- For Firebird 3.0 – set parameter `ServerMode=Super` and run *install_service.bat*.

Of course, you can choose the SuperServer for 2.5 or Classic architecture for 3.0 if you know what you need.

As a result of running the command file, Firebird of the selected architecture will be installed and run as a service.

You can make sure the Firebird service is installed and running in the **Services** snap-in (run `services.msc` in command prompt):

![Figure 2.19. Firebird Service.](image)

In this example, Firebird is installed in the folder `H:\Firebird\Firebird-2.5.5.26928-0_x64` and running as a service with the SuperClassic architecture.
2.4. Installing HQbird Server on Linux

To install HQbird Server Side on Linux, you need to download HQbird ServerSide for Linux with integrated Firebird from this location: https://ib-aid.com/en/hqbird-installation/


You must be root or sudoer to install HQbird on Linux!

**General prerequisites:** install java version 1.8 before installing HQbird! We recommend OpenJDK, but Oracle’s Java is also fine.

**Installation of HQbird with Firebird 2.5 on Linux**

1. Uninstall all previously installed Firebird versions before running this installer. Make sure you don’t have Firebird installed from repositories!

2. Apply execution rights to the installation package:

   ```bash
   chmod +x install_fb25_hqbird_server_2020.sh
   ```

3. Run installation script install_fb25_hqbird_server_2020.sh. It will install Firebird into /opt/firebird and HQbird into /opt/hqbird

4. By default, Firebird 2.5 is installed as Classic. We recommend to install it as SuperClassic – for this run script /opt/firebird/bin/changeMultiConnectMode.sh and choose thread

Next steps:

1. Please note that Firebird 2.5 will be installed with SYSDBA/masterkey

2. You can stop/start Firebird 2.5 with command `service firebird stop` or `service firebird start`. Check is it running with command `ps aux | grep firebird`

3. You can stop/start HQbird with command `service hqbird stop` or `service hqbird start`. Check is it running with command `ps aux | grep dataguard`

4. Run browser, and log in to HQbird FBDataGuard [http://serverurl:8082](http://serverurl:8082), with user/password = admin/strong password

5. Choose “I have HQbird Enterprise” and register HQbird with the email and password you have received from IBSurgeon Deploy Center.

6. If necessary, follow steps to setup — or see the appropriate chapter of this Guide.

**Installation of HQbird with Firebird 3.0 on Linux**

**Prerequisites:** make sure you have libtommath and ICU installed (there will be an appropriate error message if they are not installed).
Installation of HQbird

1. Uninstall all previously installed Firebird versions before running this installer.

2. Apply execution rights to the installation package:

   chmod +x install_fb30_hqbird_server_2020.sh


4. By default, Firebird 3.0 is installed as SuperServer. Keep it.

5. Firebird 3.0 will be installed with SYSDBA/masterkey.

   Next steps:
   
   1. You can stop/start Firebird 3.0 with command `service firebird-superserver stop` or `service firebird-superserver start`. Check it running with command `ps aux | grep firebird`.
   
   2. You can stop/start HQbird with command `service hqbird stop` or `service hqbird start`. Check it running with command `ps aux | grep dataguard`.
   
   3. Run browser, and log in to HQbird FBDataGuard [http://serverurl:8082](http://serverurl:8082), with user/password = `admin/strong password`.
   
   4. Choose “I have HQbird Enterprise” and register HQbird with the email and password you have received from IBSurgeon Deploy Center.
   
   5. If necessary, follow steps to setup — or see the appropriate chapter of this Guide.

**Installation of HQbird Standard on Linux**

If you have a license of HQbird Standard, or if you don’t want to change the existing Firebird installation, please run the following command:

   `install_fb30_hqbird_server_2020.sh --nofirebird`

It will install HQbird without Firebird binaries.

**Note**

Please note, that advanced features (replication, multi-thread support, encryption, authentication) require HQbird Enterprise with Firebird binaries!

**Firewall settings**

Firebird is installed on port **3050**, HQbird web interface is listening on port **8082**, and licensing interface is listening on **8765**.
These ports can be changed in `/opt/firebird/firebird.conf` *(RemoteServicePort)*, `/opt/hqbird/conf/network.properties` *(server.port)* and `/opt/hqbird/conf/license.properties` *(serverlicense.port)*.

Make sure to allow these ports in your firewall configuration.

**Attention!**

After upgrade, make sure that there is only the one copy of HQbird is running! If there are 2 copies, stop them (`service hqbird stop` for the first and `kill <process-number>` for the second instances) and start it again.

### 2.5. Upgrade existing HQbird version

HQbird installer on Windows (from v 2018R2) and on Linux (from v 2018R3) supports automatic upgrade of the configuration of already installed HQbird version 2017R2 and later.

If HQbird installer will notice the previous version of HQbird, it will ask you to confirm the upgrade, and in case of the positive answer, it will stop Firebird, HQbird and upgrade their files.

![Figure 2.20. Warning about upgrade.](image)

![Figure 2.21. Warning about restart of currently running HQbird FBDataGuard.](image)
Installation of HQbird

The configuration will be retained — it means that `firebird.conf`, `aliases.conf`, `securityX.fdb`, and HQbird configuration files will not be deleted (HQbird configuration files will be upgraded to the new configuration version).

The upgrade does not change the Windows service settings for Firebird and HQbird — it means that if you have changed “Run As” properties of the service, they will be retained.

**Note**

After upgrade on Linux Firebird and HQbird must be started manually!

**Important**

After upgrading HQbird, open the web-console and choose in the right upper corner: “Refresh HQbird web-console”. It is necessary to clean the cache of JavaScript part of the application.

Please note — if you are installing HQbird 2020 over the old version of HQbird on Windows, the dialog with installation options will be shown as disabled, because we cannot automatically upgrade from 2.5 to 3.0, and installer can only upgrade the same components. If you need a different installation, remove old version of HQbird from the computer prior installing 2020.
Installation of HQbird

2.6. Registration of HQbird

How to activate HQbird

To activate HQbird, you can either use a separate utility included in the server and administrator packages for Windows, or use the registration mechanism embedded into the HQBird Firebird DataGuard web interface (for Windows and Linux), or run any tool from the administrator software and use the built-in activation wizard.

The activation wizard looks and works the same in the tools and in the activation tool. It is enough to perform activation once on any computer that can connect to the server where HQbird ServerSide is installed.

Figure 2.22. An example of the disabled components selection dialog in case of upgrade.
You can launch the registration utility from the **Start** menu (IBSurgeon\HQbird Firebird Admin\HQbird):

![Image of registration utility](image)

**Figure 2.23. HQBird registration helper.**

If you click the **Register** button (or Re-Register for repeated registration), you will see the activation wizard:

![Image of activation window](image)

**Figure 2.24. HQBird activation window.**

After that, specify the **IP address** or the **computer name** of the server HQbird is installed on in the upper input field and click **Connect to HQbird Server**. If you started registration utility on the same computer with HQbird Server, it will be “localhost”, otherwise — some remote address.
Then enter your registration data. If you have a license, enter your e-mail address and password that you used to register with the IBSurgeon Deploy Center and click **Activate**.

**Note**

If you have no license, choose Trial license, specify your e-mail address and click **Activate**. You will be automatically registered and the password will be sent to your e-mail address.

Right after you click **Activate**, the registration wizard will try to connect to the IBSurgeon Deploy Center () and obtain a license. If it succeeds, you will see the corresponding message. If there are any problems, you will see the error message.

If you forget the password, click the **Forgot password...** button and it will open the browser with the password recovery form.

If you need to purchase a new or additional license or renew your subscription, click **Purchase**.

Click **Close this window** after the registration is over.

**Internet Activation via a Client Computer**

If the server with HQbird Server does not have access to the Internet, you can still activate it via the Internet: you can install HQbird Administrator on any client computer with Windows that has both access to the Internet and access to the HQbird Server and perform activation.
Run HQbird Register tool and enter there: IP address of your server (or, server name — for example, mylinuxserver), email and license, and click Activate:

![HQbird activation window](image)

**Figure 2.25. HQBird activation window.**

**Offline Activation**

If the server and all client computers have no access to the Internet, you should use offline activation. To do it, click Offline activation tab and follow instructions there. In case of any troubles please contact.
Activation in web interface

Figure 2.26. Activation in web interface.
3.1. Initial configuration of HQbird
FBDataGuard (backups, monitoring, alerts, etc)

Please follow these steps:

1. Make sure that you have Firebird 2.5.5 or later (Firebird 2.1 is also supported with some limitation), and it is working;

2. HQbird FBDataGuard service is installed and running
   a. You can check it using Services applet in Control Panel (right-click on “My Computer”, choose “Manage”, then “Services and Applications”, “Services” and find in the list “FBDataGuard Agent”)
   b. At Linux you can check it with command `ps aux | grep dataguard`.

3. Make sure the FBDataGuard port is accessible (8082) and it is not blocked by firewall or any other antivirus tools. If necessary, adjust port in FBDataGuard configuration file (see Web-console port).

Launch web-console

To open web-console type in your browser or use IP address of your server with installed HQbird ServerSide.

Or you can choose in “Start” menu IBSurgeon\HQbird Server Side\Firebird DataGuard\"Launch the DataGuard web console for localhost".

Supported browsers

FBDataGuard web interface works correctly with Firefox, Chrome, Safari and Internet Explorer 11.

Error message regarding webs-site certificate

If you have configured FBDataGuard to use https, the browser will indicate that this web-site () is not safe, and it will recommend leaving web-site. This message is caused by the default security certificate for FBDataGuard web-console.

Please ignore this message and click to open FBDataGuard web-console.

It will ask you for username and password (login dialog can be different for Firefox, Safari or Chrome).
Figure 3.1. Enter username and password for FBDataGuard web-console.

Attention!

Default username/password for HQbird FBDataGuard is "admin"/"strong password" (without quotes).

Auto discovery feature of FBDataGuard

At the first launch FBDataGuard will check computer for installed Firebird servers. FBDataGuard for Windows search registry for Firebird records, FBDataGuard for Linux checks default locations of Firebird installations.

FBDataGuard will show the list of all Firebird copies installed, but only the one instance of Firebird can be monitored by FBDataGuard. Choose it by clicking Add Firebird engine to monitoring >>

If you don’t see Firebird instance in auto discovery list, you can choose Add custom >> and configure instance parameters manually.
Configuration of HQbird

**Figure 3.2. Auto discovery feature of HQbird.**

**Firebird server registration**

To register auto-discovered server, you need to click at **Add Firebird engine to monitoring>>** and then adjust auto-discovered settings.

**Note**

Note: to use Windows Trusted Authentication (by default it's off), you need to be sure that libraries `jaybird30.dll` and `fbclient.dll` (from appropriate Firebird version) are in searchable Windows paths.

When installing under Windows, if the option to automatically register the master/replica is selected, the server will be added automatically. In this case, you can skip this step. If the option to automatically register a replica is selected, then the database will be added in addition.

Let's consider what can you see in the Server dialog (and, normally, you don't need to change them):

- **Installed in**: Firebird installation folder
- **Binary folder**: Firebird bin folder (for Firebird 3 on Windows Binary folder is the same as the installation folder)
- **Log**: location of `firebird.log`
- **Configuration file**: location of `firebird.conf`
- **Aliases**: location of `aliases.conf` or, for Firebird 3, `databases.conf` (please change it manually, if needed)
- **Host**: name of the server, usually localhost
Configuration of HQbird

- **Port**: network port for Firebird, according to `firebird.conf` settings
- **Use trusted auth**: use trusted authentication, by default it is off
- **SYSDBA login**: name of SYSDBA user, usually it is SYSDBA
- **SYSDBA password**: password for SYSDBA
- **Output directory**: Folder where backups, statistics and gathered logs will be stored

**Figure 3.3. Register server in HQbird FBDataGuard.**

By default “Output directory” for Firebird server is `${agent.default-directory}/${server.id}`, it corresponds to `C:\HQbirdData` in case of a default installation.

It can be not very convenient, so we recommend pointing FBDataGuard output directory to more simple path, usually located at disk where backups are intended to be stored, for example `F:\myserverdata`.
After clicking “Register” FBDataGuard will populate default configurations files and immediately start analysis of firebird.log. It can take a while (for example, 1 minute for 100Mb firebird.log). After that you will see initial web-console with registered Firebird server:

Figure 3.4. HQbird FBDataGuard with registered Firebird server.

FBDataGuard shows alerts and statuses of monitored objects: if everything is fine, it shows green signs, otherwise there will be yellow or red notifications.

Below we will consider in details each monitored objects and its settings.

Note

Note: you cannot delete registered Firebird server in FBDataGuard web-console. The only way to unregister server is to delete its configuration files. In general, there is no reason for deleting registered server, until you want completely uninstall FBDataGuard.

Now we let's proceed with a database registration.
Firebird database registration

To register database in FBDataGuard, you need to click at the symbol “Settings” in the right corner of “Databases” (there will be a hint “Add database to monitoring”) and fill the following form:

- “Database nick name” is for your convenience, it is used to refer this database in alerts and email messages.
- “DB alias” is a database alias from aliases.conf or in databases.conf. If you specify both “DB Alias” and “Path to database”, “DB Alias” will be used.
- “Path to database” is the local path to database (remember that FBDataGuard should work at the same computer with Firebird). If you are putting database on external drive, it can raise error “File… has unknown partition”. To fix it you need to click on “Configure” at Server widget and click “Save” to make FBDataGuard re-read partitions.
- “Crypt key name” – if the database is encrypted, specify encryption key name.
- “Crypt key value” – if the database is encrypted, specify encryption key value.
- “Output directory” is the folder where FBDataGuard will store backups, logs and statistics for this database. If you do not select HQbirdData folder during the installation, and if you do not specify output folder for the server, it's a good idea to specify “Output directory” to some explicit location like F:\mydatabasedata.

**Note**
You can specify exact absolute locations for backups and statistics later in appropriate dialogs.

You can see the list of databases available for registration or their aliases by clicking on the link View database aliases.
Figure 3.6. Available database aliases.

You can see the list of databases available for registration or their aliases by clicking on the link View open databases.

After registration, FBDataGuard will populate database configuration with default values and then show web-console with registered database:
Figure 3.7. HQbird FBDataGuard web console after adding a database.

You can adjust database settings later; now let's proceed with alerts setup.

**Email alerts in HQbird FBDataGuard**

FBDataGuard can send alerts by email to administrator(s); such alerts contain information about successful backups and potential and real problems with databases.

It's a good idea to enable setup email alerts. To do this you need to click on server name (computer name) in the top of the web-console:
After that you will see the configuration dialog for alerts:

![Alerts configuration dialog](image)

**Figure 3.8. Email alerts configuration dialog in FBDataGuard.**

First of all, you need to enable alerts sending by enabling checkbox “Send alerts by e-mail”.

- **Installation name** is some readable name for your convenience; it will be referred in emails and alerts.
- **Installation GUID** is a service field; there is no need to change it.
- **Web console background color** – often it is useful to adjust the color of HQbird web interface to distinguish them easily.
• “Send alerts to the HQbird Control Center” - if you have subscription to HQbird Control Center for Firebird, enable this checkmark to monitor status of your servers there.

• “Send alerts by email” - enable email alerts and configure email settings below.

• “Send alerts to” specifies where to send emails.

• “From field” is what will be set as sender in the email.

• “SMTP server address”, “SMTP server port”, “SMTP server login” and “SMTP server password” are data which will be used to send emails.

• “Anti-spam delay” specifies delay on sending repeating messages. It avoids flooding of administrators' mailbox with repetitive messages. 60 minutes is an optimal value.

Note
Please note: if you are using smtp.gmail.com, use port 587 and enable login of third-party applications in the settings of Gmail account.

Click “Save” to save email alerts settings.

Note
There can be delay while saving, since FBDataGuard is checking the settings and send test email to the specified address.

Next steps with FBDataGuard

After you have setup HQbird FBDataGuard and added there server and database(s) to be monitored, you need to adjust settings for the most important maintenance activities: backups, sweep and performance monitoring.
3.2. Monitoring and maintenance configuration in FBDataGuard

Overview of web-console.

Parts of web-console.

- **Dashboard** – it is the main tab where administrator can configure HQbird FBDataGuard and see server and databases statuses.
- **Alerts** – contains the full list of alerts, generated by FBDataGuard.
- **Registration** – license and registration/activation information.
- **Graphs gallery** – performance graphs.
- **Performance** – performance monitoring settings and performance reports.

Jobs

Web-console is intended for easy configuration of activities (called “jobs”) which are fulfilled by HQbird FBDataGuard.

Almost all FBDataGuard jobs have 2 purposes: the first is to monitor for some values and to raise alerts if necessary, and the second is to store historical values into logs, so later it's possible to see the dynamics of important parameters of Firebird server and database.

In this section we will consider general configuration of jobs parameters, but not an analysis of gathered logs.

Jobs widgets

General approach is the following: each activity is represented by a “widget”, which has the following parts:
Configuration of HQbird

Figure 3.9. Elements of FBDataGuard web-console widget.

Status — it is indicated with color icon and name. Status of database is a summary of all included server-level jobs and databases' statuses, and, respectively, status of database is a summary of all database-level jobs.

Status types

CRITICAL means problems, OK means “Everything is fine”, WARNING means some issues which require attention, MAJOR means major issue, MINOR – minor issue, MALFUNCTION means that jobs was not succeeded (something prevents its execution), NOT_AVAILABLE means that job is not available in this server or database version.

OFF means that job is not active, UNKNOWN means that job is active but was not started yet, so actual results are unknown.

Job name indicates the name of activity.

Configuration button opens configuration dialog, which is individual for each job.

Resolved is the link to flush the status to UNKNOWN and forgot errors which were discovered previously. The status will be updated according the current situation after the next execution of the job.

Last run shows the time after the last run of this job.

Period/Schedule to run shows how often or when the job will be started.

More>> is the link which opens the widget and shows more details and suggested action for administrator to resolve the situation.

All jobs in FBDataGuard have default settings, which are very close to recommended values for the 80% of Firebird installations, so after initial configuration server and database will be protected at
Configuration of HQbird

pretty good level comparing with default installation, however, we recommend additional configuration and tuning for every job. In the next sections we will consider each job and its configuration.

**Server: Active server**

Server: Active server widget shows summarized status of all server-level jobs and statuses of monitored databases.

![Active server](image)

**Server: Active server** also indicates Firebird currently running or not and shows detailed version of Firebird and HQbird.

If you click on configure link, you will see the same dialog that we have used to register Firebird instance in FBDataGuard, and now it can be used for changing Firebird instance properties:
In general, there is no need to edit Firebird server details after the registration, until you are not reinstalling Firebird – but in this case we recommend reinstalling HQBird too.

**Server: Auto updates**

Auto updates: OK [scheduled 0 0 22 ** ? ] [Last run: 26 Oct, 22:00:03]

Auto update is an important job which notifies you that newer version of HQbird FBDataGuard is available and suggests to update the software.

It provides an alert regarding available updates and appropriate download link. Default time to run this job is 22-00 everyday (for information).
In the configuration dialog of auto-updates you can disable auto check or set another time for it.

In fact there is a small confusion here: auto update does not perform automatic update of HQbird, it just checks for the new versions periodically, and optionally download it.

The upgrade is initiated by the administrator.

**Server: Agent Output Folder**

“Agent output folder” monitoring is intended to watch space occupied by reports, logs, stats, metadata repository and other data, gathered and generated by HQbird – this folder by default is C:\HQbirdData\output.
For databases unattended for a long time (1-2 years) it is possible that FBDataGuard logs will occupy too much space and lack of space can lead to database outage. To prevent it for sure, “Agent output folder” is watching for occupied space.

By default “Agent output folder” job is enabled.

Also, if someone has ignored recommendations to put backups’ folders to the explicit locations, it is possible that database backup will be created inside Agent folder. In this case you’ll see CRITICAL status immediately — FBDataGuard will recognize and warn you regarding wrong configuration.

And, this job is useful for bundles of FBDataGuard and third-party applications.

In the configuration dialog you can enable/disable this job, set check period (by default it is 10 minutes), and set thresholds for alerts.

Thresholds can be set in % of max size occupied by log or using the explicit size in bytes.

FBDataGuard checks both values and raises alert for the first threshold. If you wish to set % only, you need to set -1 as value to “Max occupied”.

![Agent disk-space monitoring](image)

**Server: Replication Log**

![Server log](image)

If you are using HQbird Enterprise, FBDataGuard can check replication.log for errors. In case of error it sends an appropriate alert (by email) to the administrator.

To enable this job please check “Enabled”.
Configuration of HQbird

Replication log monitoring

- **Check period** – how often to check `replication.log` for changes
- **Size to roll, bytes** — if `replication.log` will exceed will value, it will be renamed according date-time pattern
- **Date pattern for rolling** – how to rename `replication.log`
- **Keep NN error messages**: how many errors will be stored in the list of the recent errors.

**Server: Server log**

“Server log” job periodically checks `firebird.log` and if it detects that file was changed, log analysis starts. The embedded analytic engine checks each entry in `firebird.log` and categorizes them into several categories with different levels of a severity. According the severity of messages status of job is assigned and appropriate alerts are generated.

Once administrator has reviewed errors and alerts (and performed necessary actions to solve the reason of error), he need to click on “Resolved” link and FBDataGuard will forget old error messages in `firebird.log`.

In the configuration dialog of “Server log” you can enable/disable this job and set the check period (in minutes).
Also this job watches for the size of firebird.log and if its size exceeds “Size to roll”, FBDataGuard will split firebird.log and rename it according to the date-time pattern.

**Server: Temp files**

“Server: Temp files” job is useful to catch and solve performance problems with Firebird database.

While performing SQL queries Firebird stores intermediate results for sorting and merging data flows in temporary files, which are allocated in specified TEMP locations. FBDataGuard shows at “Server: Temp files” widget information about quantity and size of temporary files.

FBDataGuard recognizes locations of TEMP folders and monitors quantity and size of temporary files. Lack of space can lead to the performance problem or more serious errors, too many (or too large) temporary files can indicate problems with SQL queries quality.
Using configuration dialog you can enable/disable this job, set period and thresholds to the maximum size of temporary files (size of all files) and quantity.

If you see that size of temp files is too high and if there is enough RAM on the server, increase `TempCacheLimit` parameter in `firebird.conf` to fit all temporary tables into RAM.

Also, HQbird checks other temp files used by Firebird — if you see extreme values (several Gb) for trace or monitor, the good idea will be check the FIREBIRD_TMP folder for outdated files (with old modification timestamps). Please note — the screenshot below is not a real alert (i.e., values are Ok), it was created to demonstrate the output in case of large temporary files.

**Server: Firebird server folder**

“Firebird server folder” jobs monitors size, occupied by Firebird installation. It's enabled by default.
Configuration of HQbird

There are several threats prevented by this job: maladministration issues when database volumes or external tables are being created in %Firebird%\Bin folder, very big firebird.log which can exhaust all places at drive with Firebird installation, and some other problems.

Also this job monitors and analyses information, gathered by all space-related jobs (including database-level jobs). At the picture below you can see quick representation of space analysis for all drives where Firebird, databases and backups are stored.

Using configuration dialog you can enable/disable this job, set period of checking and thresholds for server folder size.

By default we use 200 Mb is a standard setting for Firebird installation.

If the size of your Firebird is larger, please consider clean-up of old logs and other unwanted artifacts, or increase parameter Max occupied (in bytes) to prevent false alerts.

Note for Linux users: if you see red warning regarding the inconsistent space information, add locations with database and backups to Disk Space widget:
You can get idea where is your database and backup is actually located with command `df -h`.

**Database: General configuration**

FBDataGuard can monitor several databases at the single server (up to 80 databases). For each database the separate widget is created. At the top widget database status is shown, database nickname (it’s specified during database adding and can be changed). Also database widget shows the full path to the database, its size, status of backups and the number of currently connected users.

Using configuration dialog you can set database nickname, path to database and output folder for the database (to store logs and jobs results).

FBDDataGuard checks the validity of path to database and it does not allow specifying the wrong path.

Also, for HQbird Enterprise, in the database widget you can see status of the replication and configure replication by clicking on the icon. Please read more details in the replication configuration section.

Since HQbird 2020, the database widget in HQbird also shows the encryption status of the database.

**Database: Transactions**

“Database: Transactions” job is intended to log transactions activity. It monitors 2 important intervals: difference between Oldest Active Transaction and Next transaction and gap between Oldest Snapshot and Oldest Interesting.

If these intervals are out of the frames of the specified threshold, it means problem with transactions management.
These logs can be analyzed to get helpful insight regarding database performance and application quality (see more information here http://ib-aid.com/en/articles/ibanalyst-what-you-can-see-at-summary-view/).

This job also monitors the implementation limit in Firebird: maximum transactions number in Firebird versions before 3.0 should be less than $2^{32}-1$.

Near this number database should be backup and restored. It will throw an alert if transaction number will be close to the restrictions. Also, the transaction dynamics is shown on the tab “Graphs gallery”:

**Database: Lockprint**

“Lockprint” job monitors the information from the lock table of Firebird. It is very important for architectures Classic/SuperClassic and useful for SuperServer.
The lock table is an internal Firebird mechanism to organize access to the objects inside Firebird engine. HQbird monitors the important parameters of the lock table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check period, minutes</td>
<td>3</td>
</tr>
<tr>
<td>Deadlock Scans threshold</td>
<td>12345</td>
</tr>
<tr>
<td>Deadlock threshold</td>
<td>0</td>
</tr>
<tr>
<td>Mutex Wait threshold</td>
<td>18</td>
</tr>
<tr>
<td>Hash Slots is less than</td>
<td>2047</td>
</tr>
<tr>
<td>Min length is more than</td>
<td>1</td>
</tr>
<tr>
<td>Average length is more than</td>
<td>6</td>
</tr>
<tr>
<td>Owners limit</td>
<td>700</td>
</tr>
<tr>
<td>Free owners limit</td>
<td>1000</td>
</tr>
<tr>
<td>Lock table size</td>
<td>40000000</td>
</tr>
<tr>
<td>Warn if page buffers in database header more than [NNN]</td>
<td>10000000</td>
</tr>
</tbody>
</table>

- **Check period**, minutes — how often HQbird analyses lock table. 3 minutes is an optimal interval.
• **Deadlock Scans threshold** — deadlock scan is a process, started by Firebird engine, in case of a long response delay from the one of the threads. If a number of deadlock scans is high, it means that Firebird is heavily loaded. The value is accumulated since the Firebird engine start. The default value is pretty big – 12345, so if it is exceeded, it means that database performance is poor.

• **Deadlock threshold** — if Firebird engine finds the true deadlock during the deadlock scans, it increases this value. Please note: true deadlocks are very seldom. Don't confuse them with transactions' conflicts (“deadlock. Lock conflict on nowait transaction” etc).

• **Mutex wait threshold** — Mutex Wait is a parameter of lock table which implicitly indicates the conflicts for the resources. The higher mutex wait, the more competition exists inside the engine for the resources. By default, the mutex wait threshold is set to 18%, but this value is not universal for all databases. The good approach is to watch for the mutex values during 1-2 weeks and then set the highest value seen during this period. Mutex wait graph is available in Mutex Wait gallery.

![Mutex Wait Graph](image)

• **Hash slots alerts**. Lock table header has a parameter “Hash lengths (min/avg/max): 0/0/4”, it shows the lengths in the lock table. It is important to keep these values as low as possible, so HQbird monitors them and suggest, how to improve the situation, if hash length is more than specified in this job.

• **Owners limit**. “Owners” is a number of connections established to the specified database. In fact, this is the fastest way to get the actual number of connections to the database with the minimum load to the database — other ways like request to MONSATTACHMENTS or `isc_tpb_database` have various disadvantages. The limit here should be set according the actual peak number of connections. For example, if you are sure that peak number of the connections to your database is 500, set 550 as Owners limit, and if at some moment the load will increase, you will not miss that moment.
• **Free owners.** "Free owners" is the value between the peak number of owners and current number of owners. If you see Free owners = 0, it means that number of connections grows steadily since the Firebird start. If you see high number of Free owners, it can be a sign that many connections were disconnected recently.

• **Lock table size.** The lock table size is an implicit indicator of the load to the system. Normally, lock table size should be stable. Also, it is recommended to set the initial lock table size to the value it has after some active work period — though the lock table is enlarged on demand, the re-allocation process is a heavy operation and can lead to micro-freezes in database responses. Lock table graph is useful to determine the proper initial value.

• **Lock table queue.** Lock table queue does not have the explicit threshold in Lockprint job, but its values are collected and shown in “Graphs gallery”. Lock table queue is an indicator of a general load.
Database: Index statistics recalculation

“Database: Index statistics recalculation” is an important job which helps to keep performance of indices at optimal level, and performs additional checking of a database health.

“Database: Index statistics recalculation” allows to run re-computing of indices selectivity values. During this procedure Firebird quickly walks through leaf pages of indices, and renews statistics about selectivity. By visiting these pages Firebird also verifies their integrity and if index is corrupted, the warning will be thrown.

Also, this job verifies that all indices are active in database. Inactive or non-activated indices usually indicate corruption and lead to performance degradation.

By default this job is disabled, but we recommend enabling it after careful selecting of indices for the recalculation.

There are three modes in this job: AUTO, ALL, SELECTED.

ALL is the mode where all indices will be checked.

AUTO is the default mode. It is very similar to ALL, but it also checks the size of database and do not touch indices if database is bigger than 3.6Gb.
SELECTED is the recommended mode. It allows choosing of indices which should be recomputed or those which should be avoided.

To include indices into the list of recomputed, you need to specify indices names (divided by comma), and to exclude – perform the same in the appropriate field.

As you can see at configuration dialog screenshot, there are fields to enable/disable job, to set update mode, and to include or exclude indices. “DB size to switch, bytes” is to set limit where AUTO mode is working. “Check index activity” switch should be always on, until you are not performing special manipulations with inactive indices.

**Database: Verified Backup**

“Database: Verified Backup” is one of the key jobs to guarantee the safety of data stored in the protected database. During the development of HQbird we had in mind certain recovery scenario, and this scenario implies that the key goal of database protection is to minimize potential losses of data. If we have healthy backup, recovery can be concentrated on saving the most recent data (just entered into the database), and it greatly decreases the time of overall outage.

As you will see below, “Database: Verified Backup” is not just a wrapper for standard gbak functionality and scheduler, this is a smart job which has many built-in rules to prevent problems with backups and provide suitable interface for backups management.

**Important**

“Database: Verified Backup” is disabled by default, but we strongly recommend reviewing of its settings immediately after HQbird setup.
Initially “Database: Verified Backup” job is shown as Ok, though backup was not tried. In this case OK means that backup at least scheduled.

Also this job recognizes files according the name pattern (see below information regarding configuration), and shows the totals number of backups.

After the backup will be done, the widget information will be changed: creation time of last successful backup will be shown, and also the time took to actually perform the backup (only 1 minute 12 seconds at the screenshot with example).

Also, the detailed alert will be send to your email and/or HQbird Control Center:

“Database: Verified Backup” checks the free space at the drive with backup destination, and if it detects that there is not enough free disk space, CRITICAL alert will be sent, and current backup will be canceled (if necessary).
Note

Be careful – by default backup time is set to 23-00 Monday-Sunday.

By default, database backups will be stored into the output folder that you have specified during installation step! By default, it is C:\HQbirdData\output\...

It is very important to carefully review database backups settings and adjust them according the local configuration!

Let’s consider the configuration dialog for backup in more details:

• “Enabled” is obvious – it enables or disables scheduled backups

• In the “Schedule” field you can set the time when backup should be run. Scheduler uses CRON expression and this is a right place to apply all the power of CRON (see CRON Expressions).

• “Backups folder” specifies the folder to store backups. This folder should be at the same computer where database is. By default, it is situated inside database default directory. Usually it’s a good idea to set the explicit path to the folders with backups.

• “Maximum number of backup files in folder” specifies how many previous backups should be stored. FBDataGuard stores backups in revolver order: when the maximum number will be reached (i.e., 5 backups will be created), FBDataGuard will delete the oldest backup and create the new backup. In combination with CRON expressions it gives a powerful ability to create necessary history of backups.

• “Backup name pattern” specifies how backup files will be named. Also this name pattern allows FBDataGuard to recognize old backups with the same name pattern.

• “Backup extension” is fbk by default.

• “Compress backups” specifies should FBDataGuard archive backups after regular Firebird backup. By default, this option is on, but you need to know that FBDataGuard will zip backups’ files which are less than 100 Gb in size. After that size, the backup compression will be automatically switched off. We recommend to turn this feature on for small databases only.

• “Check restore” is an important option. If it is on (by default), FBDataGuard will perform test restore of fresh backup, in order to test its validity. It guarantees the quality of created backup and notifies administrator in case of any problems with test restore.

• “Remove restored” specifies should FBDataGuard delete restored database. By default it is OFF, so you might want to turn it ON, but you need carefully consider – do you really need to keep the copy of test restored database. With each test restore this copy will be overwritten.

• “Use multiple cores to backup and test restore” - this feature is for HQbird Enterprise only, it allows to backup database and restore test database using multiple CPU cores, so backup can be made 3-5 times faster. We recommend to allocate ½ of CPU cores,

• “Send “Ok” report” – by default it is off, but it’s strongly recommended to turn it ON and start to receive notifications about correct backups. This feature will use email settings from alerts system
If we will click on button **More>>**, the advanced backup options will appear:
Configuration of HQbird

- **“Max total job duration, minutes”** - time frame to complete all backup steps. Sometimes backup process can hang up, so exceeding of the maximum time will immediately notify administrator of some problems. Also, if backup took too much time, it can indicate problems with garbage collection or abnormal growth of database itself.

- **“Backup (gbak) timeout, minutes”** - maximum time to complete only backup (gbak -b) operation, otherwise alert will be generated.

- **“Final destination folder for backups”** - if you need to make backups into the one folder, and then move created backup to another folder (for long-term storage, for example), you can change the value of this parameter from ${backup-directory} to the folder where you will keep them. Backup files in both locations are watched by HQbird FBDataGuard, and included into the count of backup copies shown in the widget.

- **“Copy backup”** switch and **“Copy backup to”** path. If you have network location or plugged USB drive to store database where you want to store copy of backup (in addition to usual backups), FBDataGuard can copy the latest backup there: just turn on “Copy backup” switch and specify “Copy backup to” path. The copied files are not monitored and not included into the number of backup files shown in the widget.

- **“Execute shell command”** switch and **“Shell command”** path. It is possible to specify custom script or executable after the general backup procedure will be complete. Shell command gets as the path to the fresh database backup as a parameter.
Configuration of HQbird

- “Optional path to gbak executable” - it is possible to specify other gbak tool than standard gbak.
- “Backups option for gbak” - if you need to add some specific options, add them here.
- “Restore options for gbak” - if you need to add specific options for test restore, add them here.

**Tip**

If you are monitoring more than one database, it is highly recommended to split the runtime of the restores.

**Important Note: Backup to the network locations**

Please be aware that for creating and copying backup to the network locations Firebird and FBDataGuard services must be started under the account with sufficient rights. By default, Firebird and FBDataGuard are started under LocalSystem account, which does not have rights to access network location.

So, to store Firebird backups to the network location on Windows, run Services applet (services.msc) and on the tab Log On change “Log on as” to the appropriate account (Domain Admin should be fine).

For Linux – add necessary rights for “firebird” user.

**Database: Incremental Backup**

Incremental backup is a job to schedule and manage incremental backups in Firebird.

Please note that we recommend to use incremental backups only in combination with verified backups, since incremental backup performs coping of database pages changed since the last backup (in case of multilevel incremental backup).

HQbird FBDataGuard implements 2 types of multilevel incremental backup: Simple and Advanced incremental backups, and also Dump backup (see Database: Dump backup).
Multilevel backup in Firebird must follow the following steps:

1. Create initial backup (level 0) which essentially is the copy of the database at the moment of backup start and mark it with backup GUID.

2. Since Firebird marks each data page with a certain identifier at every change, it is possible to find data pages, changed from the moment of previous backup and copy only them to form backup of level 1.

3. It is possible to create several level of the backups – for example, the initial backup (full copy, level 0) is being created every week, every day we create level 1 (differences from the level 0), and at every hour we create level 2 backups (differences from daily level 1).

Incremental backup with simple schedule allows planning 3 levels of backups: weekly, daily and hourly.

You can see summary information for such incremental backup configuration at the following screenshot of its widget:

![Incremental backup](image)

Incremental backup: **UNKNOWN**
- Level 0 - Files: 1; Occupied size: 112.9 Gb
- Level 1 - Files: 5; Occupied size: 10.4 Gb
- Level 2 - Files: 3; Occupied size: 1.7 Gb

Latest backup
- Level0: 20160408_022212+20160413_050212.nb1 (112.9 Gb)
- Level1: 20160408_022212+20160413_050212.nb1 (2.9 Gb)
- Level2: not yet done

In order to setup Simple incremental backup, click on Settings “gear” of the widget and select “Simple schedule” (selected by default). The following dialog will appear:
Configuration of HQbird

There are 4 main areas in this dialog, let's cover them one by one.

The top area is devoted for general settings of the incremental backup – they are the same for Simple and Advanced schedules:

**Max duration, sec** – it limits the maximum duration of backup process, by default is 1 day (86400 seconds).

**Minimum free disk space (bytes)** – minimal size of free disk space to prevent backup to start, by default ~9Mb

**Backup folder** – where incremental backup for the selected database will be stored. It is necessary to store incremental backups for each database separately from backups of other databases: i.e., the separate folder for each database.
Configuration of HQbird

It is necessary to specify backup folder with enough free disk space to store all level of backups!

**Journal name**—file name details information about incremental backups files, for internal use only.

**Path to nBackup** – it is possible to specify other nbackup tool than standard nbackup (not recommended).

**Backup name pattern** – pattern for files of incremental backup (no need to change it).

**Options** – additional options for nbackup command line tool (no need to change it).

**Do not check existence of backup files** – this option should be checked if you plan to delete or more incremental backups to another location.

**Do not check GUID chain** – this option should be checked if you want to skip existence check of previous levels of incremental backups.

**Immediately create non-existing low-level backups** – by default this option is On. It means that if you have scheduled the initial start moment of level 1 backup earlier than the initial start moment of level 0 backup, DataGuard will automatically fix it and create level 0 backup right before level 1. The following backups of level 0 will be fulfilled according the regular schedule.

**Send OK email for levels 0, 1, 2** – enable this option to receive notifications about incremental backups *(highly recommended!)*

After setting main set of parameters the schedule itself should be set. As you can see on the screenshot below, you need to specify day of the week and time to do level 0 (weekly) backup, days of week and time to start level 1 (daily) backups and hours and minutes of level 3 (hourly backups).

For each backup level you can specify how many files to keep in history.
Configuration of HQbird

By default it is set to keep 5 weekly backups, 7 daily and 24 hourly backups. However, sometimes more flexible schedule is required, for this purpose Incremental Backup widget has Advanced schedule:

As you can see, the upper part of the configuration screen is the same as in Simple schedule, and the difference is in the way how backup levels are scheduled.
Advanced schedule allows to setup up to 5 levels of backup, and plan them with flexible CRON expressions.

For example, you can setup it to create full copy (level 0) backup every 3 months, level 1 copy every month, level 2 – every week, level 3 every day and level 4 – every hour.

**Tip**

If you are monitoring more than one database, it is highly recommended to split the runtime of the backups.

**Database: Dump Backup**

This job also utilizes nbackup functionality in Firebird, but unlike multilevel backups, it always performs a full copy (level 0) of the database. Such job is useful to quickly create a copy of working database.

The configuration of Database: Dump backup is trivial:

![Config Form](image)

You just need to setup when and where DataGuard should copy a full copy (level 0 incremental backup), and how many copies it should keep.

**Database: RestoreDB**

One of the often tasks of the database administrators is restoring database from the backup. There could be many reason to do restore, the most popular reasons are regular check of the stored backups.
and necessity to have fresh restored copy for quick rollback. HQbird FBDataGuard can automate restoring of backups (which were created with gbak or Database: Verified backup) with **Database: RestoreDB** job. Let’s consider the options and parameters of this job.

![RestoreDB](image)

**RestoreDB**

OST    31 min 16 sec ago
Recent restored database: H:\TEMP\ba...stextend.fdb(8.5 Gb)
Restored from backup: H:\TEMP\ba...418_14.25.fbk(18/04/2016 14:25)
Restore time: 8 min 51 sec
By default, restore is disabled – and, since restoring can be long and resource-consuming job, please plan when to restore carefully. Below you can see the configuration dialog for **Database: RestoreDB**: 
### Restore Database / dbmaster

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Scheduled</td>
<td>0 22 4 * MON-FRI</td>
</tr>
<tr>
<td>Get backup from folder</td>
<td>${db.default-direcory}/backup</td>
</tr>
<tr>
<td>Restore from nbackup chain using date pattern</td>
<td>[0.date,yyyyMMddHHmms]</td>
</tr>
<tr>
<td>Template for gbak backup file name</td>
<td>backup_{0.date,yyyyMMdd_HH-mm}</td>
</tr>
<tr>
<td>Backup gbak file extension</td>
<td>.fbk</td>
</tr>
<tr>
<td>Take date of gbak backup from</td>
<td>File name</td>
</tr>
<tr>
<td>Take backup not older than, hours</td>
<td>24</td>
</tr>
<tr>
<td>Remove old source (backup) files, keep only</td>
<td>0</td>
</tr>
<tr>
<td>Restore to directory</td>
<td>${backup-directory}</td>
</tr>
<tr>
<td>Restore with file name</td>
<td>${db.id}_{0.date,yyyyMMdd_HH-mm}_testrestore.fdb</td>
</tr>
<tr>
<td>When existing database found</td>
<td>Rename existing file</td>
</tr>
<tr>
<td>Append suffix to file name</td>
<td>{0.date,yyyyMMdd_HH-mm}.old</td>
</tr>
<tr>
<td>Execute command after restore</td>
<td></td>
</tr>
<tr>
<td>Use NN CPU cores to restore</td>
<td>N/A</td>
</tr>
<tr>
<td>Restore (gbak) timeout, minutes</td>
<td>480</td>
</tr>
<tr>
<td>Check available space before restore. Minimum value (bytes)</td>
<td>10000000</td>
</tr>
</tbody>
</table>

**Notify on successful restore**

**Cancel** | **Save**
**Configuration of HQbird**

- **“Scheduled”** field contains CRON expression which defines when to run restore.

- **“Get backup from folder”** - specify the location of backup file(s) to be restored. If you are restoring backups at the same computer where they have been created, specify the same folder as it is in Database: Verified backup job. If you are restoring backups from the another computer, specify the folder where those backups are located.

- **“Template for backup file name”** contains the template for backup names. It should be the same as for the backup.

- **“Backup file extension”** - by default it is fbk.

- **“Take backup not older than, hrs”** - this parameter specifies the maximum age of backup to be restored. If the latest backup file will be older than specified number of hours, RestoreDB job will send the alert with warning that backup is too old. This is useful for automatic checking of backups created on the remote computer.

- **“Restore to directory”** - folder where FBDataGuard will restore backups.

- **“Restore with filename”** - template for the restored database file. By default it contains the following parts:
  - ${db.id}_{0,date, yyyyMMdd_HH-mm}_testrestore.fdb
  - Db.id – internal identifier of the database (GUID)
  - 0,date, yyyyMMdd_HH-mm – timestamp
  - testrestore.fdb – description (You can set there any filename you need).

- **“When existing database found”** - if FBDataGuard will encounter a file with the same name as restored database in the destination folder, by default it will rename the existing file. If you want to replace old restored file with new one, choose “Replace existing file”.

- **“Append suffix to filename when rename”** - if you have chosen “Rename existing file”, this suffix will be used to rename it. If you have chosen “Replace existing file”, this suffix also will be used to rename, but after that the old file will be deleted.

- **“Execute command after restore”** - in this field you can specify an optional path to the command file or another utility to be started after the restore. There will be 2 parameters passed: the first is the path to the backup which was just restored, and the second is the path to the restored file.

- **“Use multiple cores to restore”** - specify number of cores for parallel restore (available only in HQbird Enterprise 2020)

- **“Limit restore process time, minutes”** - here you can set the time limit for restore operation. If this limit will be exceeded, the warning will be sent, saying that restore takes too long.

- **“Check available space before restore (bytes)”** - here you can set the limit for the minimal free space in the restore destination – if there is less free space than specified, restore will not start, and associated warning will be sent.

- **“Notify on successful restore”** - send email about successful restore (by default it is off, only alerts about problems will be sent).
**Database: Transfer Replication Segments**

The purpose of "Transfer Replication Segments" job is to send replication segments produced by async replication from master to replica server. In the case of distributed environment of the asynchronous replication, when the network connection between master and replica server is unstable, or with high latency, or when servers are in the different geographical regions, the best way to transfer replication segments will be through FTP or FTP over SSH.

Below we will consider how to setup Transfer Replication Segments for this task.

First, the asynchronous replication master should be configured to save replication segments into the some local folder – by default, it will be $\{\text{db.path}\}.\text{LogArch}$ – as it is shown in the example below:

- **Replication role**: Master
- **Working mode**: Asynchronous
- **Log directory**: $\{\text{db.path}\}.\text{RepILog}$
- **Log archive directory**: $\{\text{db.path}\}.\text{LogArch}$
- **Optional parameters**:
  - `exclude_without_pk=true`
  - `log_segment_count=54`

Find and exclude tables without Primary or Unique keys

Reinitialize replica database

See initialization status
Then we can setup Transfer Replication Segments job to monitor this folder for the new replication segments and upload them to the remote FTP server.
Configuration of HQbird

As you can see at the screenshot above, Transfer Replication Segments job checks folder, specified in “Monitor this folder” with an interval, specified in “Check period, seconds”. Please note – Transfer Replication Segments sends files in the order of their names, not dates.

To check that transferred files are valid replication segments, and to support automatic re-initialization of the replica databases, the checkmark “Enable/disable replication cloud backup job” must be enabled.

By default, Cloud Backup compresses and encrypts replication segments before send them. The default password is “zipmasterkey” (without quotes), which can be specified in the field “Compress with optional password”. FBDataGuard creates the compressed and encrypted copy of the replication segment and upload it to the specified target server.

To disable packing and encryption, uncheck the “Compress with optional password” checkmark.

**FTP/FTPS/FTPS over SSH**

There are several types of target servers: FTP, FTP over SSL/TLS, FTP over SSH. When you select the necessary type, dialog shows mandatory fields to be completed.

You can select up to 5 simultaneous remote servers to upload backups. Below you can see the configuration dialog for FTP.

<table>
<thead>
<tr>
<th>FTP/FTPS/FTPS over SSH</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note 1: If you don't have FTP installed on the target server with Windows, install Filezilla – it is very popular fast and lightweight FTP-server for Windows.</td>
<td></td>
</tr>
</tbody>
</table>
**Note**

Replication segments will be uploaded to the subdirectory specified in the “Upload to folder”. By default, this is `/database0/${db.id}`, where `db.id` is the identifier of the database inside the DataGuard. The replica about this `db.id` does not know anything, so you need to register it manually in “Unpack to directory” (see File Receiver).

---

**FTP over SSL/TLS**

In order to send files to FTPS, it is necessary to create jks storage with private key file, and specify path to it in the field “Key store file” and password for it in “Key store password”.

See details and example how to create jks file and password here: [http://xacmlinfo.org/2014/06/13/how-to-keystore-creating-jks-file-from-existing-private-key-and-certificate/](http://xacmlinfo.org/2014/06/13/how-to-keystore-creating-jks-file-from-existing-private-key-and-certificate/)

The last part of parameters in Transfer Replication Segments dialog allows controlling the behavior of Transfer Replication Segments.

- **Delete local prepared copy** – by default it is On. This parameter specify that Transfer Replication Segments job deletes compressed copy of the replication segment after the successful upload to
the target server. If you don't want to keep these copies on the master server, keep the parameter enabled.

- **Delete local prepared file copy** – by default is Off. It means status means that replication segment will be not deleted by FBDataGuard after uploading. It can be useful if you want to keep the full history of changes in replication segments, but, be careful; in case of an intensive write activity replication segments can occupy a lot of space (Terabytes).

- **Send Ok report** – send email to the specified in Alerts address every time when replication segment is uploaded. By default it is off.

As a result, FBDataGuard will upload encrypted and compressed replication segments to the remote server. To decompress and decrypt them into the regular replication segments, another instance of HQbird FBDataGuard should be installed on the replica server, and File Receiver job should be configured – see more details in the section Database: File Receiver.

**FTP over SSH**

To use FTP over SSH with private key authentication, please specify the full path to it in "Key store file", other parameters are similar to usual FTP.

**Database: Transfer Files**

The purpose of "Transfer Files" job is to send backup files from master to replica server. In the case of distributed environment, when the network connection between master and replica server is unstable,
or with high latency, or when servers are in the different geographical regions, the best way to transfer files will be through FTP or FTP over SSH.

Below we will consider how to setup "Transfer Files" for this task.

First, the database server should be configured to save backup files into the some local folder — by default, it will be `${db.default-directory}/backup` — as it is shown in the example below:

![Transfer Files configuration](image)

**Figure 3.11. Transfer Files configuration**
Then we can setup **Transfer Files** job to monitor this folder for the new backup files and upload them to the remote FTP server.

As you can see at the screenshot above, **Transfer Files** job checks folder, specified in “Monitor this folder” with an interval, specified in “Check period, seconds”. Please note – Transfer Files sends files in the order of their names, not dates.

By default, Transfer Files compresses and encrypts backup files before send them. The default password is “**zipmasterkey**” (without quotes), which can be specified in the field “**Compress with optional password**”. FBDataGuard creates the compressed and encrypted copy of the backup and upload it to the specified target server.

To disable packing and encryption, uncheck the “**Compress with optional password**” checkmark.

**FTP/FTPS/FTPS over SSH**

There are several types of target servers: FTP, FTP over SSL/TLS, FTP over SSH. When you select the necessary type, dialog shows mandatory fields to be completed.

You can select up to 5 simultaneous remote servers to upload backups. Below you can see the configuration dialog for FTP.

![Transfer Files / dbmaster / FTP 1](image)

**Note**

If you don't have FTP installed on the target server with Windows, install Filezilla – it is very popular fast and lightweight FTP-server for Windows.
**Note**

Replication segments will be uploaded to the subdirectory specified in the “Upload to folder”. By default, this is `/database0/${db.id}`, where `db.id` is the identifier of the database inside the DataGuard. The replica about this `db.id` does not know anything, so you need to register it manually in “Unpack to directory” (see File Receiver).

---

**FTP over SSL/TLS**

In order to send files to FTPS, it is necessary to create jks storage with private key file, and specify path to it in the field “Key store file” and password for it in “Key store password”.

See details and example how to create jks file and password here: [http://xacmlinfo.org/2014/06/13/how-to-keystore-creating-jks-file-from-existing-private-key-and-certificate/](http://xacmlinfo.org/2014/06/13/how-to-keystore-creating-jks-file-from-existing-private-key-and-certificate/)

The last part of parameters in Transfer Files dialog allows controlling the behavior of Transfer Files.

- **Delete local prepared copy** – by default it is On. This parameter specify that Transfer Files job deletes compressed copy of the file after the successful upload to the target server. If you don't want to keep these copies on the master server, keep the parameter enabled.
Configuration of HQbird

- **Delete local prepared file copy** – by default is Off. It means status means that file will be not deleted by FBDataGuard after uploading. It can be useful if you want to keep the full history of changes in files, but, be careful; in case of an intensive write activity such files can occupy a lot of space (Terabytes).

- **Send Ok report** – send email to the specified in Alerts address every time when replication segment is uploaded. By default it is off.

- **Perform fresh backup** – disabled by default. Transfer Files remembers the last number of file it sends. If you need to start again from scratch, from file 1, enable this parameter. Please note that it will automatically become disabled after the resetting of the counter.

As a result, FBDataGuard will upload encrypted and compressed files to the remote server. To decompress and decrypt them into the regular files, another instance of HQbird FBDataGuard should be installed on the replica server, and File Receiver job should be configured – see more details in the section *Database: File Receiver.*

**FTP over SSH**

![Transfer Files / dbmaster / FTP 1](image)

To use FTP over SSH with private key authentication, please specify the full path to it in “Key store file”, other parameters are similar to usual FTP.

**Sending verified and incremental backups through Transfer Files**

Transfer Files also can be used to send any files to FTP/FTPS/etc. For example, you can setup Transfer Files to look for FBK files, produces by Verified Backup Job, and schedule to upload to the remote FTP server.
It is necessary to remember that number of stored backups should be less than the number of files to be preserved by Transfer Files (specified in the parameter “How many files to keep”). By default, Transfer Files keeps 10 last sent files, and Verified backup has 5 most recent backup files, so it works. Ok, but if you will reduce the number of kept files in Transfer Files, it will delete extra files according to “Filename template”.

The same can be done for incremental backups.

**Database: File Receiver**

In general, File Receiver is designed to decompress files from zip archives, and the most often it is used in the pair with Cloud Backup to transfer archived replication segments.

File Receiver checks files in the folder specified in “Monitor directory”, with interval equal to “Check periods, minutes”. Its checks only files with specified mask according to “Filename template” (*.arch* by default) and specified extension (.replpacked by default), and if it encounters such files, it decompresses and decrypts them with the password, specified in “Decrypt password”, and copies to the folder, specified in “Unpack to directory”.

If parameter “Monitor for replication” is enabled, File Receiver also will check that received file is actually a replication segment (it has specific header), and if it is not, it will raise an appropriate warning.
There are the following additional parameters:

- **Alert if number of unpacked files more than** – by default is 30. If there is a long queue of replication segments to be unpacked, it can be a problem with a replica database, so HQbird sends alert to attract administrator’s attention.

- **Warn if the newest file in unpack folder is older than (minutes)** – if the most recent file (usually, replication segment) is too old (more than 360 minutes), the replication process can be broken, and HQbird sends an appropriate alert.

- **Send Ok report** – by default it is Off. If it is On, HQbird sends an email about each successful unpacking of the segment. It can be too often for replication segments, because they are arriving every 30-180 seconds, and Ok for normal files like verified or incremental backups.

- **Perform fresh unpack** – disabled by default. Cloud Backup Receiver remembers the last number of replication segment it unpacked. If you need to start unpacking from scratch, from segment 1 (for example, after re-initialization of replication), enable this parameter. Please note that it will automatically become disabled after the resetting of the counter.
Configuration of HQbird

After setup of File Receiver, configure the replica to look for replication segments: set in the “Log archive directory” the same path as in “File Receiver” -> “Unpack to directory”.

Embedded FTP server

HQbird has embedded FTP server, which is off by default. It is suitable to use embedded FTP server to receive replication segments.

In order to enable embedded FTP server, it is necessary to edit the `ftpsrv.properties` configuration file, which is located in `C:\HQbirdData\config` or `/opt/hqbird/ftpsrv.properties`.

By default, it contains the following:

```
#path in ftpsrv.homedir must be escaped "ftpsrv.homedir=c:\\ftp\\pub"
# or backslashed for ex: "ftpsrv.homedir=c:/ftp/pub"
ftpsrv.enable = false
ftpsrv.port = 8721
ftpsrv.defuser=admin2
ftpsrv.defpsw=strong password2
ftpsrv.homedir=
```

It is necessary to change `ftpsrv.enabled` to `true` and specify the home directory for FTP in `ftpsrv.homedir` parameter. Also, it is recommended to use non-default username and password.
After that, restart FBDataGuard service, and check availability of the FTP.

**Attention — Linux users!**

On the Linux, FBDataGuard service runs under firebird user, so FTP home directory also should have permission for user firebird.

---

**Database: Low-level metadata backup**

“Database: Low level metadata backup” is one of the key jobs of DataGuard, it ensures database protection at low level.

First of all, this job stores raw metadata in special repository, so in case of heavy corruption (due to hardware failure, for example) of database it is possible to use this repository to recover database.

The second purpose of this job is to constantly check all important system tables for consistency. Every 20 minutes it walks through all important system tables in the database and ensures that there are no errors at metadata level.

The third purpose is to warn administrator about too many formats for each tables.

There is an implementation limit in Firebird to have 256 formats per table, however even several formats can greatly increase a chance of hard corruption and can slow down the performance. It is recommended do not change tables structure at production database and keep only one format per each table. If it’s not possible, administrator should try to perform backup/restore more often to transform all formats into the single one.

---

**Database: Validate DB**

Validation of Firebird database requires exclusive access: i.e., no users should be connected during validation. “Database: Validate DB” job shuts down the database and performs validation of database, and then turns it on.
By default, this job is OFF. Please consider carefully, is it possible to provide exclusive access for database. Validation can also take significant time.

Using configuration dialog, you can enable/disable this job, set time to run, set the shutdown timeout (time to wait before launch validation), and also shutdown mode (FORCE, ATTACH, TRANSNATIONAL). If you have no deep knowledge in what you are doing, it's better to keep default parameters.

“Database: Validate DB” will send alert with critical status if there will be any errors.

Also, Firebird will write errors into firebird.log, and they will appear in the alerts generated by “Server log” job.

**Database: Sweep Schedule**

FBDataGuard includes special job to run an explicit sweep, in case if automatic sweep was disabled. By default, job is disabled.

The recommendation is to schedule explicit sweep with disconnection of long-running transactions for all databases where such transactions are detected. The recommended period is once per day (usually during the night, after backup’s completing).

By default, sweep is set to 23-00, which can be not a good time, because default verified backup starts at the same time, so better change it.
Configuration of HQbird

Please note: by default, check mark “Disconnect all connections with long-running active transactions before sweep” is enabled. It means that HQbird will find and disconnect long-running transactions (more than 30 minutes) before sweep — in order to make sweep efficient. If long-running active transactions will be not disconnected, sweep cannot clean old records versions.

“Do not disconnect processes with name pattern” — in this parameter specify SIMILAR TO expression for processes names which will be not disconnected. By default, we exclude gbak, gstat and fbsvcmgmr processes.

“Disconnect all processes older than (minutes)” — HQbird will disconnect processes which have long-running active writeable transactions, by default threshold is 30 minutes. The practical upper limit for this parameter is 1440 minutes (it is highly unlikely that transaction does something useful more than 1 day).

“Use multiple cores to sweep” — HQbird Enterprise can use multiple cores to perform sweep operation, in order to make sweep 4-6 times faster. We recommend to specify no more than 1/2 CPU cores in case of the single database on the server, or 1/4 of CPU cores if there are several databases. For example, if you have 16 cores and 1 big database, set this parameter to 8, if there are several big databases, set 4.

**Database: Delta**

If you are using incremental backups (or Dump backup), this job is critically important. It watches for delta-files lifetime and size, and warns if something goes wrong. Forgotten delta-files are the often reason of corruptions and significant losses of data.
This job finds all delta files associated with database and check their age and size. If one of these parameters exceeds thresholds “Maximum delta size” or “Maximum delta age”, administrator will receive the alert and database status will be set to CRITICAL.

**Note**

If delta file of the protected database was corrupted, it is possible to extract data from it using metadata from the original database file or repository from “Low-level metadata backup” job.

### Delta file monitoring / test

| **Check period, minutes**: | 5 |
| **Maximum delta size, bytes**: | 52428800 |
| **Maximum delta age, minutes**: | 360 |

### Database: Disk space

This job watches for all objects related with database: database files (including volumes of multi-volume database), delta-files, backup files and so on.

“Database: Disk space” job analyzes the growth of database and estimate will there be enough free space for the next operation like backup (including test restore) on the specific hard drive.

It generates several types of alerts. Problems with disk space are in the top list of corruption reasons, so please pay attention to the alerts from this job.

This job also contributes data to the server space analysis graph ( ).

By default, this job is enabled.

Using configuration dialog, you can specify check period and thresholds for free space. The first reached threshold will be alerted. To set threshold only in % of disk space, you need to set explicit space in bytes to 0.
Database: Database statistics

This job is very useful to capture performance problems and perform overall check of database at low-level without making backup.

We recommend running this job every day and storing a history of statistics report.

Then, with HQbird Database IBAnalyst it is possible to find problems with database performance and get useful recommendations how to fix them.

**Note**

As a useful side effect, gstat visits all database pages for tables and indices, and ensures that all of them are correct.
**Database: SQL Ping**

SQL Ping job is an easy yet powerful diagnostic tool: it runs an SQL query with a specified schedule (by default CRON expression is set to run every 5 minutes):

![SQL Ping settings](image)

*Figure 3.12. SQL Ping settings*

The default SQL query is `select count(*) from rdb$types, rdb$types, rdb$types;` and default threshold to generate the alert is 1000 ms for execution, 500 ms for connection time and 500 ms for the disconnect.

To make this job more useful, it is recommended to use the SQL query which is relevant for the database: it should be a read-only query which is frequently used by the client applications; in this case the slowness of its execution will mean that database is less responsive than it should be.

There are 2 possible usage of this job: 1) it sends alert if the ping SQL exceeds the threshold, 2) HQbird draws the graph with the response time, so you can see the history of database response.
3.3. FBDataGuard tips&tricks

FBDataGuard allows changing its setting not only through web-console, but also using direct modification of configuration files. This can be useful when you need to install FBDataGuard in silent mode (no interaction with user), to bundle it with third-party software, or to perform some fine configuration adjustments.

Path to FBDataGuard configuration

During the start FBDataGuard looks for in registry for configuration and output paths:

![Registry Editor screenshot]

These values specify the paths to FBDataGuard configuration and output folder — these values are chosen during installation.

Adjusting web-console port

One of the most frequently asked questions is how to adjust port for web-console application (by default it is 8082), It can be done by changing port setting in file `%config%/agent/agent.properties` (%config% is `C:\HQbirdData\config` or `/opt/hqbird/conf`).

```sh
server.port = 8082  #change it
```

%config% - folder to store configuration information, it is specified in .

How to change password for Admin user

You can specify its password in the file `access.properties` (in `C:\HQbirdData\config` or `/opt/hqbird/conf`)

```sh
access.login=admin
access.password=youradminpasswordforhqbird
```
After setting the password, restart FBDataGuard, and new password will be encrypted and applied.

**Guest user for HQbird FBDataGuard**

There is read-only user to access HQbird FBDataGuard, with the name guest.

```plaintext
access.guest-login=guest
access.guest-password=yournewpassword
```

### 3.4. Appendix: CRON Expressions

All jobs in FBDataGuard have time settings in CRON format. CRON is very easy and powerful format to schedule execution times.

**CRON Format**

A CRON expression is a string comprised of 6 or 7 fields separated by white space. Fields can contain any of the allowed values, along with various combinations of the allowed special characters for that field. The fields are as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Mandatory</th>
<th>Allowed Values</th>
<th>Allowed Special Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds</td>
<td>YES</td>
<td>0-59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Minutes</td>
<td>YES</td>
<td>0-59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Hours</td>
<td>YES</td>
<td>0-23</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of month</td>
<td>YES</td>
<td>1-31</td>
<td>, - * / L W</td>
</tr>
<tr>
<td>Month</td>
<td>YES</td>
<td>1-12 or JAN-DEC</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of week</td>
<td>YES</td>
<td>1-7 or SUN-SAT</td>
<td>, - * / L #</td>
</tr>
<tr>
<td>Year</td>
<td>NO</td>
<td>empty, 1970-2099</td>
<td>, - * /</td>
</tr>
</tbody>
</table>

So cron expressions can be as simple as this: * * * * ? * or more complex, like this: 0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010

**Special characters**

* ("all values") — used to select all values within a field. For example, "*" in the minute field means "every minute".

? ("no specific value") — useful when you need to specify something in one of the two fields in which the character is allowed, but not the other. For example, if I want my trigger to fire on a particular day
of the month (say, the 10th), but don't care what day of the week that happens to be, I would put “10” in the day-of-month field, and “?” in the day-of-week field. See the examples below for clarification.

- — used to specify ranges. For example, “10-12” in the hour field means “the hours 10, 11 and 12”.

, — used to specify additional values. For example, “MON,WED,FRI” in the day-of-week field means “the days Monday, Wednesday, and Friday”.

/ — used to specify increments. For example, “0/15” in the seconds field means “the seconds 0, 15, 30, and 45”. And “5/15” in the seconds field means “the seconds 5, 20, 35, and 50”. You can also specify “/” after the “character — in this case ” is equivalent to having “0” before the “/”. “1/3” in the day-of-month field means “fire every 3 days starting on the first day of the month”.

L (”last”) — has different meaning in each of the two fields in which it is allowed. For example, the value “L” in the day-of-month field means “the last day of the month” — day 31 for January, day 28 for February on non-leap years. If used in the day-of-week field by itself, it simply means “7” or “SAT”. But if used in the day-of-week field after another value, it means “the last xxx day of the month” — for example “6L” means “the last Friday of the month”. When using the “L” option, it is important not to specify lists, or ranges of values, as you'll get confusing results.

W (”weekday”) — used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify “15W” as the value for the day-of-month field, the meaning is: “the nearest weekday to the 15th of the month”. So if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However, if you specify “1W” as the value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not “jump” over the boundary of a month’s days. The “W” character can only be specified when the day-of-month is a single day, not a range or list of days.

# — used to specify “the nth” XXX day of the month. For example, the value of “6#3” in the day-of-week field means “the third Friday of the month” (day 6 = Friday and “#3” = the 3rd one in the month). Other examples: “2#1” = the first Monday of the month and “4#5” = the fifth Wednesday of the month. Note that if you specify “#5” and there is not 5 of the given day-of-week in the month, then no firing will occur that month.

Note

The “L” and “W” characters can also be combined in the day-of-month field to yield “LW”, which translates to “last weekday of the month”.

Note

The legal characters and the names of months and days of the week are not case sensitive. MON is the same as mon.

CRON Examples

Here are some full examples:

<table>
<thead>
<tr>
<th>Expression</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 12 * * ?</td>
<td>Fire at 12pm (noon) every day</td>
</tr>
</tbody>
</table>
### Configuration of HQbird

<table>
<thead>
<tr>
<th>Expression</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 15 10 ? * *</td>
<td>Fire at 10:15am every day</td>
</tr>
<tr>
<td>0 15 10 * * ?</td>
<td>Fire at 10:15am every day</td>
</tr>
<tr>
<td>0 15 10 * * ? *</td>
<td>Fire at 10:15am every day</td>
</tr>
<tr>
<td>0 15 10 * * ? 2005</td>
<td>Fire at 10:15am every day during the year 2005</td>
</tr>
<tr>
<td>0 * 14 * * ?</td>
<td>Fire every minute starting at 2pm and ending at 2:59pm, every day</td>
</tr>
<tr>
<td>0 0/5 14 * * ?</td>
<td>Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day</td>
</tr>
<tr>
<td>0 0/5 14,18 * * ?</td>
<td>Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day AND fire every 5 minutes starting at 6pm and ending at 6:55pm, every day</td>
</tr>
<tr>
<td>0 0-5 14 * * ?</td>
<td>Fire every minute starting at 2pm and ending at 2:05pm, every day</td>
</tr>
<tr>
<td>0 10,44 14 ? 3 WED</td>
<td>Fire at 2:10pm and at 2:44pm every Wednesday in the month of March</td>
</tr>
<tr>
<td>0 15 10 ? * MON-FRI</td>
<td>Fire at 10:15am every Monday, Tuesday, Wednesday, Thursday and Friday</td>
</tr>
<tr>
<td>0 15 10 15 * ?</td>
<td>Fire at 10:15am on the 15th day of every month</td>
</tr>
<tr>
<td>0 15 10 L * ?</td>
<td>Fire at 10:15am on the last day of every month</td>
</tr>
<tr>
<td>0 15 10 ? * 6L</td>
<td>Fire at 10:15am on the last Friday of every month</td>
</tr>
<tr>
<td>0 15 10 ? * 6L 2002-2005</td>
<td>Fire at 10:15am on every last Friday of every month during the years 2002, 2003, 2004 and 2005</td>
</tr>
<tr>
<td>0 15 10 ? * 6#3</td>
<td>Fire at 10:15am on the third Friday of every month</td>
</tr>
<tr>
<td>0 0 12 1/5 * ?</td>
<td>Fire at 12pm (noon) every 5 days every month, starting on the first day of the month.</td>
</tr>
<tr>
<td>0 11 11 11 11 ?</td>
<td>Fire every November 11th at 11:11am.</td>
</tr>
</tbody>
</table>

**Important**

Pay attention to the effects of ‘?’ and ‘*’ in the day-of-week and day-of-month fields!

**Notes**

Support for specifying both a day-of-week and a day-of-month value is not complete (you must currently use the ‘?’ character in one of these fields).

Be careful when setting fire times between mid-night and 1:00 AM - “daylight savings” can cause a skip or a repeat depending on whether the time moves back or jumps forward.

More information is here [http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html](http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html)
3.5. Configuring firebird.conf for the best performance

HQbird includes set of optimized configuration files for all Firebird versions from 1.5 to 3.0 – they are located in HQBird\Configurations.

If you did not perform a justified tuning of firebird.conf or you are using default firebird.conf, consider to use one of the optimized files from this collection.

There are three variants of Firebird configuration files for every Firebird architecture: balanced, read-intensive and write intensive. We always recommend to start with balanced firebird.conf. Then we recommend to measure actual ratio between reads and writes using HQbird MonLogger tool (tab “Aggregated Performance Statistics”). In 90% of cases there are much more reads than writes, so the next step is to try read-optimized firebird configuration file.

Firebird configuration greatly depends on the hardware, so if you want to tune Firebird properly, please also read “Firebird Hardware Guide”, it will help you to understand what parameters must be tuned.

For the deep tuning of high-load Firebird databases IBSurgeon offers Firebird Database Optimization Service: https://ib-aid.com/en/firebird-interbase-performance-optimization-service/

Also, HQbird FBDataGuard analyses the database health and sends alerts with intelligent suggestions to increase specific parameters in firebird.conf, like TempCacheLimit or LockHashSlots.

Attention!

If you have specified many page buffers in the header of your database and installed SuperClassic or Classic, it can affect Firebird performance. To avoid the potential problem, set page buffers in the header of your database to 0, it will ensure that the value from firebird.conf will be used:

gfix -buff 0 -user SYSDBA -pass masterkey disk:\path\database.fdb
4.1. Monitoring with HQbird FBDataGuard

Overview

HQbird monitors all aspects of Firebird server and database functioning, and includes continuous monitoring and detailed monitoring.

The continuous monitoring is performed by HQbird FBDataGuard. It is low-invasive, but very effective monitoring which can help to find and resolve the majority of issues with databases performance and stability.

FBDataGuard performs the following monitoring activities:

- Optional performance monitoring with TraceAPI and MON$
- Monitoring of transactions markers dynamics (Next, OAT, OIT, OST, active transactions)
- Monitoring of lock table activity (queues, deadlocks, mutexes)
- Monitoring of Firebird log (errors, warnings, messages)
- Number of connected users
- Free space monitoring for server, databases and their backups
- Health monitoring through analysis of database metadata and general availability of server and databases
- Number and size of Firebird temporary files (sorting, etc)
- Indices monitoring: health and activity check
- General validation of Firebird database
- Backups statuses monitoring

FBDataGuard can graphically represent information gathered during the monitoring, for example, transactions and number of users:
In the version 2020, HQBird introduces the new approach for the automatic performance monitoring with Firebird MON$ tables and TraceAPI.

Now it is possible to schedule the regular check of database performance for every HQBird (Standard, Professional, Enterprise) in less than 1 minute.

For this just open tab Performance and setup monitoring for transactions and queries:
In order to setup Performance monitoring, specify its mandatory parameters in the dialog:

The first mandatory parameter is “Enable performance monitoring” — it must be enabled to run traces by schedule.

The next important parameters are “Start trace session at” and “Stop trace session”. They contain CRON expressions which specify when tracing starts and stops.

**By default, trace is set to start at 10-30 and to end at 11-00.** It is recommended to adopt tracing schedule for your needs. Below you can see the table with some popular options.

<table>
<thead>
<tr>
<th>CRON expression for Start</th>
<th>CRON expression for End</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 * ? * *</td>
<td>0 10 * ?* *</td>
<td>Run trace every hour from 0 to 10 minutes</td>
</tr>
<tr>
<td>0 0 8 ? * *</td>
<td>0 0 17 ?* *</td>
<td>Run trace every day from 8-00 to 17-00</td>
</tr>
<tr>
<td>0 30 10,13,15 ? * *</td>
<td>0 0 11,14,16 ? * *</td>
<td>Run trace sessions every day from 10-30 to 11-00, 13-30 to 14-00 and from 15-30 to 16-00</td>
</tr>
</tbody>
</table>

The next important parameter is time threshold for the slow queries, it is set in the field “Log SQLs with execution time more than”. In this field you need to set time threshold (in milliseconds), after exceeding it logs will be stored and analyzed.

By default, the time is set to 1000 milliseconds, or 1 second. It means, that only queries which take more than 1 seconds, will be logged and analyzed.

We recommend keeping 1000 ms as a basic value, until your database is very slow: in this case 3000-5000 ms can be a good start.

“Send email” check mark indicates if there necessity to send the performance report. The email settings from Alerts configuration will be used to send performance report.

For more advanced settings, “Performance Monitoring” dialog has additional parameters (normally, you don' t need to adjust them).
• "Configuration template" — name of the configuration template file which should be used for trace settings

• "Database filter" — how the database should be identified. Usually AUTO is enough, it will trace specified database. In case of Filename or Alias it will use filename or alias to filter database events. «Manual» provides an ability to set any regular expression, to trace several databases, for example, or more than one alias for the single database.

• "Database name filter" it is used in case of “MANUAL” selection.

• "Trace format" — AUTO means automatic selection, 2.5 or 3.0 will force format for 2.5 or 3.0. Usually there is no need to change it.

• "Keep recent reports" — it specifies how many reports should be kept in the “Output folder” for possible retrospective usage.

As a result of this job, HQbird will generate the performance report, which will be stored in the Output folder as a file with the extension html, and it will be sent by email (in case if “Send email” is enabled). Also the most recent performance is available for review and download in the HQBird interface.
What can we see in the performance report?

The HQbird FBDataGuard performance analysis provides 3 types of reports:

1. list of queries sorted by their time — “Sort by duration”;
2. list of queries sorted by its frequency — “Sort by frequency”;
3. list of queries sorted by the total time (i.e., summary execution time for queries with the same text and various parameters) — “Sort by summary”.

In the beginning of the report you will see the graphical representation of most problematic SQL queries:
When you click “Sort by duration” (it is a default option), you will see SQL queries and stored procedures which took the longest time to execute first.

Normally there will be long-running reports and other big SQLs.

When you click on “Sort by frequency” link in the header of the report, you will see most frequent queries: i.e., those queries which started frequently (among logged queries).

For example, in this case the statement SP_GETINVOICE_REPORT was run 46 times. It means that this query heavily affects the overall performance, and it should be optimized first.

When you click on Sort by summary, you will see the queries which took the most part of the time (among logged queries). These queries usually are the best candidates for the optimization.
Monitoring

**Detailed information for the problematic SQL queries**

To see details of the most frequent query, click in the link “View details” in the bottom of the query text:

```
view_details: 44deda8fde13a2d6f557f3c15f37edff7903995a
```

As a result, you will see the longest query among the queries with the same SQL text, with its execution plan, execution statistics and input parameters.

This information is enough to analyze and optimize SQL query in Firebird SQL Studio or other developer IDE.

**Automatic monitoring of long-running active transactions**

On the “Performance” tab you can find the option to enable automatic monitoring of long active transactions:
By default, this monitoring is off. To enable it, click on «Enable transactions monitoring». In general, it is enough, this monitoring does not require further setup.

Let's consider it's settings:

- **When to log transactions**: This parameter defines when to check MON$ tables for long-running active transactions. By default, it is set to run every 5 minutes (see CRON statement). You can make less often on heavy loaded databases, up to once per hour.

- **Output folder**: It is a service parameter.

- **Show transactions older then (minutes)**: It specifies the time threshold to show the transaction (and associated connection) in the list of long-running-transactions. By default, this threshold is 60 minutes: it means that writeable transactions which started more than 1 hour ago, will be considered as long-running.

- **Send alert if oldest active transaction is older then (minutes)**: The same, but it triggers alert and, if email notifications are enabled, the automatic email with the details of long running active transaction. The text of the alert looks like the following:

  There is a long running active transactions: it was started at 11/13/17 1:19 PM (and run at least 107 minutes)) from ::1/51068 by C:\HQbird\Firebird30\isql.exe. Such transactions block garbage collection, please perform transactions analysis with HQbird MonLogger.

- **Show only NN oldest active transactions**: It specifies how many records will be shown in the list with long-running transactions.

The list of long-running active transactions is shown on the screenshot below:

Here you can see that isql.exe started 2 long-running active transactions to the database h:\employee_30.fdb at November 13, 18-05.

**How to select a tool for detailed monitoring**

FBDataGuard is the first line of a defense for Firebird database; once FBDataGuard encounters something suspicious inside the monitored areas, it sends an alert with description of the issue.

**Important!**

If you have several Firebird servers, we offer HQbird Control Center application which gathers alerts data from the Firebird servers and databases and shows them at the single screen. Contact our for more details.
After receiving such alert from FBDataGuard the database administrator should proceed with detailed investigation of the problem.

The choice of tool for detailed monitoring depends on the type of detected problem.

If FBDataGuard reports long-running active transaction (Next-OAT), it is necessary to use HQbird Mon$Logger to detect the source of currently running active transaction.

If stuck of oldest interesting transaction is reported, database administrator must plan an explicit sweep to clean uncollected garbage with FBDataGuard sweep job (if it is necessary) and then plan tracking of forced rollbacks with Performance Monitoring in FBDataGuard, or, if it is an old version of Firebird (2.1 or older), with FBScanner.

If users report slowness problem with some queries, Perfusion or FBScanner should be used.

If there is unusual spikes in transaction behavior, IBTransactionMonitor can be a good addition to HQbird FBDataGuard to clarify the situation.

The problems with general database performance and occasional or periodic slowness require an analysis of database structure, which can be done only with HQbird Database Analyst.

Below we will consider how to work with HQbird monitoring tools in more details.

### 4.2. Monitoring with MON $ tables: HQbird MonLogger

HQbird MonLogger is a tool to analyze monitoring tables output in Firebird and find problems with slow SQL queries, wrongly designed transactions (long-running transactions, transactions with incorrect isolation level, etc) and identify problematic applications.

MonLogger can connect to Firebird database with performance problems and identify what is the reason of slowness: is it some user attachment, slow SQL query or long-running transaction?

MonLogger supports Firebird 2.1, 2.5 and 3.0 – for older Firebird versions or InterBase please use FBScanner.

MonLogger can show you:

- Top attachments with highest number of IO operations, non-indexed and indexed reads
- Top SQL statements with highest number of IO operations, non-indexed and indexed reads
- Problematic transactions: long-running transactions, transactions with erroneous isolation level, read/write transactions, and related information: when they started, what applications started these transactions, from what IP address, etc
- Attachments and statements with the most intensive garbage collection actions
- Read/write ratio, INSERTS/UPDATE/DELETE ratio, and more.

After connection to the database where you want to find performance problems, several snapshots of monitoring tables should be done – click on “Get Snapshot” to take snapshot.


### Aggregated performance statistics for users attachments

At the first screen we can see aggregated statistics for database connections, and identify connections with the biggest problems:

- **Sequential reads / Indexed reads**
  - "Sequential reads / Indexed reads" shows us total ratio between sequential (non-indexed) reads and indexed reads in application. Usually number of non-indexed reads should be low, so big percent of sequential reads is sign that many SQL queries have NATURAL execution plans, and they could be a reason of slow response time.
  - Click on record in “TOP attachments: sequential/indexed reads” will bring you to tab “Attachments”, where you can see more details about Attachment, and then jump to tab “Transactions” or “Statements”, where you will see transactions and attachments linked with selected attachment (if checkmark “Link to selected attachment” is on, otherwise all transactions/statements for all attachments will be shown).

- **Write details**
  - “Write details” gives you an overview of write operations: ratio between INSERTs/UPDATEs/DELETEs among all database attachments. In the table of top writers you can see attachments with the biggest...
number of write operations. It is useful to identify applications or software modules which performs excessive number of update or deletes (which are the most dangerous operations in terms of garbage collections).

**Garbage collection details**

What garbage collection operations mean?

- **Purge** — engine removes back-versions, only primary version is in database.
- **Expunge** — both primary version and all back-versions were deleted.
- **Back-out** — remove only primary version (due to rollback).

Usually we can associate purge with UPDATE operation, Expunge with DELETE, and Backout with rollback of INSERT or UPDATE. Many backouts could mean that there is a problem with transaction management in the application.

**Memory usage**

"Memory usage" graph shows us total memory used by all active attachments now, and peak of allocated memory for them in the past.

List of top attachments by memory usage shows us the biggest memory consumers among your attachments. It is useful to find applications or software modules with excessive memory usage.

**Aggregated performance statistics for statements**

At the second tab you can find aggregated performance statistics for statements.
Monitoring

This statistics better reflects the momentary situation in the database – since monitoring tables collect information since the beginning of each object life, statements you can see here are those which were running during the moment when snapshot was taken.

**Sequential reads / Indexed reads**

In this list we can see top statements which perform many sequential reads from the database. Usually such statements require SQL tuning – either through indices tuning, or through SQL query redesign.

To tune the query, check its execution plan: usually it is possible to improve query speed by eliminating `NATURAL` in plans with new indices or query redesign. Click on the statement in this list to open tab “Statements”, where you can find more details about selected statement, and jump to associated transaction or attachment.

**Page reads/page writes**

This graphs and list shows brief information about top statements which perform many reads – it means that they consume significant IO and can affect performance of other queries. SQL statements with peak values should be carefully checked for optimal performance.

**Write details for statements**

At this graph you can see what writing SQL statements were doing at the moment when snapshot of monitoring tables was taken, and identify UPDATES and DELETEs which made many changes in the database.

**Garbage collection details for statements**

At this graph we can see how many garbage collection operations were done by statements running at the moment of snapshot.

**Memory usage for statements**

Unlike aggregated memory usage statistics for attachment, statements’ memory usage can show us list of exact statements which consume a lot of memory at the moment.

**Attachments**

The third tab is “Attachments”. You can open this tab directly to jump there by clicking one of the records at “Aggregated performance statistics”.

“Attachments” shows the list of users connected to the Firebird database, with many useful details: USER and ROLE of attachment, start time and ID of attachment, is there garbage collection enabled for the attachment, name of remote process which established an attachment, and several accumulated performance counters for the attachment: number of sequential reads [done by attachment since its start], number of indexed reads, number of inserts, updates and deletes, as well records backouts, purges and expunges.

By default some of columns of attachment are switched off, to show only most important information.

Of course, every time you click on attachment, you can jump to transactions running inside it, and then to statements. There is a checkbox in the left upper corner of Transactions and Statements tabs, which controls the behavior — when checked, only transactions and statements marked by selected attachment ID, will be shown.

**Transactions**

Tab “Transactions” shows active transactions at the moment when snapshot was taken.
If checkbox “Link to selected attachment” is enabled, only transactions for selected attachment will be shown, otherwise all transactions are shown.

One of the most important characteristics is a lifetime of transactions: since Firebird is designed to work with short write transactions, it is important to keep them as short as possible. MonLogger highlights transactions with isolation modes and read-write settings which hold Oldest Active transaction and therefore provoke excessive record versions to be not cleared. If you see such transaction and it started a while ago, it means that it can be responsible for excessive records versions.

Sort on “started at” column and look for old transactions, marked in red: all writeable transactions and read only snapshots stuck Oldest Active Transaction and provoke excessive record versions to be hold. Identify where these transactions started (right-click and select “View parent attachment”) and fix your code to commit this transaction earlier.
Monitor Statements

Tab “Statements” shows statements active at the moment of snapshot: if you need to catch all statements FBPerfMon or FBScanner should be used (all these tools are part of IBSurgeon Optimization Pack).

If “Link to selected attachment” is enabled, only statements for specific attachment will be shown, otherwise all active statements are in the list.

Some statements have no associated transaction id (=0): these queries are prepared, but not executed.

4.3. Monitoring with HQbird FBScanner

What is FBScanner?

FBScanner (Firebird Scanner) is a tool included in HQbird advanced distribution of Firebird, which can monitor and view all traffic between Firebird and InterBase servers and their client applications. It shows the real-time activity of connected clients:

- Connections (IP/Name, duration, CPU load),
- Queries (query text, status, parameters)
- Transactions (with parameters).

FBScanner can log all SQL traffic to text files and external Firebird database, it includes FBScanner LogAnalyzer module to analyze SQL performance.
FBScanner can be used to profile database applications, monitor user activity, and manage database connections (including client disconnects on Classic, SuperClassic and SuperServer architectures). It’s also ideal for troubleshooting INET errors, as well as auditing existing applications and performance tuning.

FBScanner supports Firebird (V1.x, V2.0, V2.1 and V.2.5), InterBase (V4.0 to 2009/XE3). It is a useful tool for analyzing production databases, especially if the application has been developed by third-party and there is no source code available.

FBScanner is transparent as far as the database application is concerned and does not require any changes in application or database source code, logic or configuration.

**Issues that FBScanner can help to resolve**

- Real-time monitoring of connections. FBScanner shows all connections to the selected database server: the IP/DNS name of connected client, database and connection time.

- Real-time monitoring of SQL queries. For each connection FBScanner shows all the currently running SQL queries along with their transaction parameters.

- Detection of the oldest connection and the oldest active transaction to allow you to analyze that may have non-optimal transaction behavior or incorrect transaction design or show users who might be using the application in a manner that may be affecting performance.

- Client disconnects. Check that disconnections are taking place correctly. You can also use FBScanner to disconnect users in order to perform maintenance or database upgrades.

- FBScanner allows the routing of specific applications or particular users to allow you to zoom in on specific applications or users.

- You can log SQL queries. For debugging or for security FBScanner can log all the selected traffic to a special database for further analysis. FBScanner includes LogAnalyzer tool to find bad queries and ineffective SQL plans.

**Performance Impact**

FBScanner does not change anything in transferred SQL traffic and works simply like a transparent proxy, so all applications will work normally.

FBScanner consume approximately 50-150Mb of memory (for 30-100 active clients), it is known that FBScanner adds approximately 150ms for every SQL statement.

**How to configure FBScanner for local computer?**

To configure FBScanner start “FBScanner Service Settings” from Start menu (IBSurgeon\HQbird Server Side\Firebird SQL Scanner\). This tool will help you to setup both basic and advanced configuration parameters for FBScanner.

The basic configuration parameters are shown at the main screen of “FBScanner Configuration”. It scans Windows registry for installed Firebird services and show them in the grid.
Monitoring

By default Firebird uses port 3050 for network connections. FBScanner works as a transparent TCP proxy – it redirects all SQL traffic from and to Firebird clients to another.

FBScanner offers to change Firebird port to 3053, in order to start its own instance at 3050. FBScanner checks for the port usage and if either 3050 or 3053 are used by other software (not Firebird), it will warn you with red caption “Port used” near new “Port” text box.

The green figure in the center of “FBScanner Configuration” main screen briefly shows how client applications SQL traffic will be passed.

At the figure below you can see that FBScanner found Firebird 1.5 instance, and offers to change its port to 3053, in order to set own instance to listen at 3050.

Such default scenario will give the maximum compatibility with existing Firebird clients (i.e., end-user applications).

To approve the changes, click “Ok”, otherwise “Cancel”.

Important

If FBScanner settings were changed, FBScanner Service will be restarted, and all existing Firebird connections will be dropped! Be careful with changing FBScanner settings in production environment. FBScanner will ask your permission to restart, please decide carefully.

How to setup FBScanner for remote computer?

FBScanner can route SQL traffic not only as local proxy, but from another computer too. To understand the difference and discover consequences, let's walk though details.

The basic (and default) configuration of FBScanner implies that it works on the same computer where Firebird is working, and process all SQL traffic from Firebird clients (i.e., end-user applications) which use default connection string (and, therefore, port 3050).
Sometimes it's not convenient to setup FBScanner to process all requests, for example, in case of:

- Only several (may be, the single workstation) workstations need to be profiled/logged
- Only certain application or narrow functionality need to be profiled
- Developers need to check some SQL code on the live database — gather SQL log with execution statistics, plans, etc.
- Heavy load (too many workstations). In case of heavy load FBScanner can consume resources of the main server, and it’s better to move FBScanner (as well as FBScanner log, if it's enabled, to the dedicated computer).
- Linux server. If Firebird works on Linux, it's possible to route SQL traffic through remote instance of FBScanner on Windows.

In these cases the good idea is to setup FBScanner at the remote computer and pass only part of SQL traffic through it. It also makes possible to perform necessary analysis of SQL without changing ports or other configuration at server — the only needed adjustment will be change host name in client applications’ connections strings.

One of the frequent use cases for setting up FBScanner in remote configuration is using it as debug console for developer computer, so developer can see in real-time (with FBScanner LogViewer) or afterwards (with FBScanner LogAnalyzer) all SQLs from own computer to the Firebird server.

At the figure below you can see how it can look like:
Now let's back to the configuration and see how easy to setup FBScanner to route SQL traffic at the remote computer.

At the bottom of the main screen of “FBScanner Configuration” you can see the following default settings (for Firebird 2.5 example we considered above):

In order to setup FBScanner to route SQL traffic to the remote Firebird, we need to change “Server Type” from “Local…” to “Remote”. It will change the main screen of the configuration tool.

First of all, we need to specify network name (or IP) of the computer with Firebird instance and port where it will be used — it should be entered into “Interface” text box.

Then we need to specify Firebird version – in our example it's Firebird 1.5.

FBScanner instance also has “Interface” — it's the list of network adapters found at the computer. If you need to bind FBScanner to one of them and disable connections from other network adapters, choose one of the adapters from the drop-down list. By default FBScanner will accept Firebird clients' requests from all network adapters.

Below you can see the example of FBScanner configuration to route SQL traffic to remote Firebird instance, which resides on myserver1 computer and works on default port 3050.
Click “Ok” to confirm new settings, and FBScanner will route SQL requests to the remote Firebird.

**Important**

If you need to pass SQL traffic from client applications through remote FBScanner, please change Firebird appropriate connection string. For example, if originally client applications have connected with "myserver1: C:\Database\data.fdb", in order to pass SQL traffic through FBScanner in this example you need to change connection string to "computer1: C:\Database\data.fdb" (where computer1 is the network name of the computer where FBScanner works).

**How to setup logging?**

From Start menu run “Firebird Scanner\FBScanner Settings”, then click button “Advanced options” (in the right bottom of the main screen).

At the dialog click tab “SQL log”.
By default logging is disabled.

**Important**

It's important to understand that logging to SQL database will write all SQL operations, including transactions, connects, etc. It means that SQL log database will consume the same amount of resources (CPU, HDD, etc) as the main database does. Due to this fact for heavy load environments we recommend to use remote configuration of FBScanner for SQL logging.

There are 2 options for logging — to file and to Firebird log database.

**Logging to text files**

File logging creates text file for each connection where FBScanner writes SQL and transactions operators. We recommend file logging for debug purposes and during development — it's suitable to investigate linear SQL code. If there are a lot of connections, file logging becomes not very suitable.

To enable file logging, click radio button near “File” option and set folder where to store file logs (check that specified folder exists first!):
Then click “Ok”.

**Important**

Enabling logging will require restart of FBScanner Service, so all current connections will be dropped. FBScanner will ask your permission to do it immediately.

**Example of text file logging**

For the following isql commands

Use `CONNECT` or `CREATE DATABASE` to specify a database

```
SQL> connect "localhost:E:\Temp\TEST15_2.FDB"
Database: "localhost:E:\Temp\TEST15_2.FDB"

SQL> create table t1(i1 integer, c1 varchar(150));
SQL> create table t2(i2 integer, b1 blob);
SQL> select count(*) from t1;
COUNT ===========
  0
SQL> insert into t1(i1, c1) values(1, 'test');
SQL> select count(*) from t1;
COUNT ===========
  1
```
SQL> exit;

FBScanner created the following log:

/* Log created by FBScanner v2.7.19
14.01.2011 16:06:07
  Client IP      = 127.0.0.1
  Client Name    = ibsurgeon3
  Client Process = isql [1884]
*/
CONNECT '127.0.0.1/3053:E:\Temp\TEST15_2.FDB' USER 'SYSDBA';

/* 14.01.2011 16:06:09 */
/* TrID=20; */
SET TRANSACTION READ WRITE WAIT SNAPSHOT;

/* 14.01.2011 16:06:09 */
/* TrID=22; isc_tpb_version1, isc_tpb_write, isc_tpb_read_committed, isc_tpb_wait, isc_tpb_no_rec_version */
SET TRANSACTION READ WRITE WAIT ISOLATION LEVEL READ COMMITTED NO RECORD_VERSION;

/* 14.01.2011 16:06:19 */
/* QrID=26 TrID=22; EXECUTE */
create table t1(i1 integer, c1 varchar(150));

/* 14.01.2011 16:06:19 */
/* QrID=26 TrID=22; INFO */
/* 14.01.2011 16:06:19 */
/* TrID=22; */
COMMIT;

/* 14.01.2011 16:06:33 */
/* TrID=27; isc_tpb_version1, isc_tpb_write, isc_tpb_read_committed, isc_tpb_wait, isc_tpb_no_rec_version */
SET TRANSACTION READ WRITE WAIT ISOLATION LEVEL READ COMMITTED NO RECORD_VERSION;

/* 14.01.2011 16:06:33 */
/* QrID=31 TrID=27; EXECUTE */
create table t2(i2 integer, b1 blob);

/* 14.01.2011 16:06:33 */
/* QrID=31 TrID=27; INFO */
/* 14.01.2011 16:06:41 */
/* TrID=32; isc_tpb_version1, isc_tpb_write, isc_tpb_read_committed, isc_tpb_wait, isc_tpb_no_rec_version */
SET TRANSACTION READ WRITE WAIT ISOLATION LEVEL READ COMMITTED NO RECORD_VERSION;

/* 14.01.2011 16:06:41 */
/* QrID=36 TrID=20; EXECUTE */
select count(*) from t1;

/* 14.01.2011 16:06:41 */
/* QrID=36 TrID=20; INFO */
126
As you can see, file log is useful to understand how SQL commands were run inside the single connect.

Logging to Firebird database

Before you start with SQL log, it's necessary to understand some implementation details, which can be important for production systems.

In general logging to Firebird database is implemented in the straightforward way: FBScanner service writes all traffic to the external Firebird database. Firebird database with log can be at the same computer where FBScanner resides, or at the remote computer.

Please consider the following requirements for SQL log configuration:

- Log database (and appropriate Firebird instance) should be in Firebird 2.5 format (since FBScanner 2.7.15). If you are forced to use FBScanner at the computer with another Firebird version, you need to use embedded Firebird 2.5 to store log.

- SQL traffic from all logged connections is written into the single table, with appropriate markers (from what computer, application, user, etc. this particular record was created).

- Log database can consume significant amount of resources in case of heavy load. For many connections it's recommended to setup FBScanner and Firebird log database at dedicated computer.
• In many cases it’s not necessary to log all connections, because they repeat the same set of SQL queries. Careful investigation of the single connection can be the most effective way to find performance problems.

To enable SQL logging, click on “SQL” radio button. It will enable appropriate text boxes and controls.

![Firebird SQL Logging Configuration](image)

First of all, click button “Edit”.

![Firebird Connection to Database](image)

**Important**

If you intend to use the same Firebird instance to log SQL traffic, you need to specify connections string with explicit and direct port. In our example it will be port 3053, and connection string looks like `127.0.0.1/3053:C:\FBScanner_log.fdb`

In this dialog you also need to specify how to connect to database with log.

If there is no database with specified name, create new database — click “Create database log”.

Test connection with log database — click “Test connection”.

Click “Ok” to save settings.
Transactions markers

FBScanner can gather information about transactions markers (in the same way like IBSurgeon Transaction Monitors does). Gathered information will be shown as graphs in FBScanner Log Analyzer.

For this purpose, FBScanner runs separate connect, which requires Login, Password and path to the appropriate client dll (if you track Firebird 1.5 with FBScanner, fbclient.dll from 1.5 will be required).

If you decide to gather transactions markers information, mark checkbox “Collect transactions counters info” and fill out Login, Password and Client DLL fields.

Using Embedded Firebird 2.5 for SQL log

If you need to use SQL log at the computer where old Firebird is used (1.0, 1.5, 2.0, 2.1 or even InterBase), it's recommended to use Firebird 2.5 Embedded to store log.

You can download Firebird 2.5 Embedded from www.firebirdsql.org.

Unpack the archive right into the FBScanner folder (C:\Program Files\IBSurgeon\Firebird Scanner by default) and rename fbembed.dll into fbclient.dll.

Folder structure will look like this

![Folder structure](image)

After that run “Advanced options”, tab “SQL logging”, radio button “SQL” and click “Edit”, then in the “Client library” point to the renamed fbclient.dll, as it shown below.
Monitoring

Tip
In Embedded Firebird fbclient.dll represents the whole engine. It works inside the process of FBScanner and there is no interaction with other installed Firebird instances, both full and embedded.

How to analyze FBScanner log?

Many users told us that they did not realize how many queries, transactions and other operations are performed by their software. As you remember, FBScanner stores all information into the single table. It uses self-links to reduce the amount of stored information and it makes raw log hard to read and understand.

To facilitate log analysis we have created new module in FBScanner — LogAnalyzer. It's available in IBSurgeon Deploy Center for all FBScanner users (inside “Download” section).

LogAnalyzer requires Firebird 2.5 to work with log database. It also creates new indices and runs heavy reporting queries, so it's recommended the following procedure:

1. Setup logging and gather statistics for at least 1 day
2. Copy log database to another computer with Firebird 2.5
3. Connect to the copy of log database and perform analysis at the developer's computers
4. Copy updated versions of log databases as necessary

To analyze log database, start LogAnalyzer and click “Connect to FBScanner log base”, then fill out connection parameters and select log database.
At first start LogAnalyzer will create necessary indices, it can take several minutes.

After that LogAnalyzer will show the last available day in the log at the “Server Load” tab:
“Server Load” tab shows how many SQL queries were run per minute, and how much time they took to execute. Effectively it shows server load, i.e., number of queries and their execution times.

Zoom in (button in the top left corner of the tab “Server load”), drag graph by holding right-button of the mouse and select the peak you are interested to investigate — click right-button to show popup-menu.

It will show you tab “All statements”, where you can browse SQL queries.

Select any query to see its text and, if plan logging feature is enabled, its plan.
To follow the execution flow, you can right-click on the query and look for connection and transactions for this query.

LogAnalyzer marks bold queries in the same transaction:
You can sort queries and, for example, find query with the longest execution time:

<table>
<thead>
<tr>
<th>ROW_TYPE_A</th>
<th>IDTRANSACTION_NUM</th>
<th>START_TIME</th>
<th>PREPARE_TIME</th>
<th>EXECUTE_TIME</th>
<th>END_TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>query</td>
<td>207407</td>
<td>186215</td>
<td>14361</td>
<td>0</td>
<td>32594</td>
</tr>
<tr>
<td>query</td>
<td>211270</td>
<td>20828</td>
<td>17338</td>
<td>0</td>
<td>30624</td>
</tr>
<tr>
<td>query</td>
<td>207518</td>
<td>201265</td>
<td>14539</td>
<td>0</td>
<td>14766</td>
</tr>
<tr>
<td>query</td>
<td>207372</td>
<td>201225</td>
<td>14392</td>
<td>0</td>
<td>14437</td>
</tr>
<tr>
<td>query</td>
<td>214522</td>
<td>186215</td>
<td>19618</td>
<td>0</td>
<td>14109</td>
</tr>
<tr>
<td>query</td>
<td>214109</td>
<td>186215</td>
<td>19176</td>
<td>0</td>
<td>13672</td>
</tr>
<tr>
<td>query</td>
<td>211668</td>
<td>186215</td>
<td>17139</td>
<td>0</td>
<td>12470</td>
</tr>
<tr>
<td>query</td>
<td>208263</td>
<td>201460</td>
<td>15296</td>
<td>0</td>
<td>11792</td>
</tr>
<tr>
<td>query</td>
<td>207597</td>
<td>186215</td>
<td>14544</td>
<td>0</td>
<td>10937</td>
</tr>
</tbody>
</table>
Monitoring

To know more about this query — double-click on it and see more details

---

**How to track 10054 errors, disconnects and failed login attempts?**

FBScanner automatically logs all 10054 errors, disconnects and failed login attempts with detailed description in the `FBScanner.log` file, which is in FBScanner main directory.

---

19.08.2010 21:43:09
Connect Error
Client IP = 192.10.1.2
Client Name =
DB Name =
DB User = MORTON
Client Process = SUPC [5520]
Client Process (by fbclient) = E:\TEMP\TEST1.EXE [5520]
STATUS = [file is not a valid database]

19.08.2010 21:43:25
Login Failed
Client IP = 127.0.0.1
Client Name = ibsurgeon3
Monitoring

<table>
<thead>
<tr>
<th>DB Name</th>
<th>= C:\Program Files\Jupiter2010\Data\data.gdb</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB User</td>
<td>= MORTON</td>
</tr>
<tr>
<td>Client Process</td>
<td>= Jupiter.exe [3032]</td>
</tr>
<tr>
<td>Client Process (by fbclient)</td>
<td>= E:\TEMP\TEST1.EXE [3032]</td>
</tr>
</tbody>
</table>
| STATUS           | = [Your user name and password are not defined. Ask your database administrator to set up a Firebird login.]

**Backup/restore and mass load operations**

To perform operations which do not require monitoring or debugging, like backup and restore or mass load of records (in billing systems) we recommend bypassing FBScanner service.

If FBScanner is installed in default recommended configuration, i.e., on port 3050 and Firebird is on port 3053, connection strings should be like this

```
server_name/3053:Disk:\Path\database.fdb
```

equivalent of connection string

```
connect "localhost/3053:C:\TEMP\database.fdb" user "SYSDBA" password "masterkey";
```

Example of using backup command

```
gbak.exe -b -g -v -user SYSDBA -pass masterkey
localhost/3053:C:\TEMP\database.fdb C:\temp\backup.gbk
```

and, of course, using local connection string will always bypass FBScanner:

```
gbak.exe -b -g -v -user SYSDBA -pass masterkey
C:\TEMP\database.fdb C:\temp\backup.gbk
```

**Real-Time Monitoring: FBScanner Viewer**

To monitor connections, queries and transaction in real-time FBScanner includes special tool namely FBScanner Viewer.

FBScanner Viewer shows momentary snapshot of SQL traffic between Firebird and monitored client applications.
In the first column we can see type of record — connection, statements or transaction.

In the table below you can find description of all columns at main page of FBScanner Viewer (some columns are hidden by default, use menu Columns to turn them on/off):

<table>
<thead>
<tr>
<th>Column title</th>
<th>Column description</th>
</tr>
</thead>
</table>
| ! (first column)   | Indicates type of record in FBScanner Viewer — there are separate set of values for SQL statements, transactions and connections. They are described in the next table below.  
Sign “!” in the title of this column means active filter — click on the triangle at right side of sign “!” to adjust it. |
| Tag                | Green/red background shows CPU Usage in % (red — Kernel, green — Firebird).  
Text is shows tags value (if it was specified in SQL query).  
Example how to set tag values:  

```sql
SELECT * FROM RDB$DATABASE  
/*FBSCANNER$CON_NAME=MyConnect;  
FBSCANNER$TR_NAME=MyTransaction;  
FBSCANNER$ST_NAME=SomeImportantQuery; */;
```

Also in this column you will see execution of gbak and gfix tools. |
| Transaction Count  | Applicable for connection row. Number of active transactions in the connection is shown.  
It's very useful to find applications with auto-commit and other ineffective transaction management issues. |
<p>| PID                | Process ID for Firebird. Only for Classic Architecture |
| Client IP          | IP of connection |
| Client Name        | DNS of connection (if possible to resolve) |</p>
<table>
<thead>
<tr>
<th>Column title</th>
<th>Column description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Process Name</td>
<td>Starting from Firebird 2.1, fbclient.dll shows name of client application. For example, C:\Program Files\Firebird\Firebird_2_1\bin\isql.exe</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority of Firebird instance (Classic only)</td>
</tr>
<tr>
<td>Database</td>
<td>Database name or its alias, as it appears in the connection string</td>
</tr>
<tr>
<td>User</td>
<td>Users name — for example, SYSDBA (it does not supported Trusted Authentication)</td>
</tr>
<tr>
<td>Role</td>
<td>Role of user</td>
</tr>
<tr>
<td>Start</td>
<td>For connection row — connection time, for transaction — start time of transaction, for statement — query start time.</td>
</tr>
<tr>
<td>Time</td>
<td>'NOW' — Start; Time from the start moment</td>
</tr>
<tr>
<td>Last Activity</td>
<td>Time of last action for current connect/transaction/statement.</td>
</tr>
<tr>
<td>Inactive</td>
<td>'NOW' — Last Activity; Period of inactivity</td>
</tr>
<tr>
<td>Latest Retaining</td>
<td>Time of the most recent “COMMIT RETAINING” or “ROLLBACK RETAINING” in the current transaction</td>
</tr>
<tr>
<td>Retaining</td>
<td>'NOW' — Latest Retaining</td>
</tr>
<tr>
<td>Received</td>
<td>Bytes, received by client</td>
</tr>
<tr>
<td>Sent</td>
<td>Bytes, sent by client</td>
</tr>
<tr>
<td>CPU Time</td>
<td>Shows overall time consumed in connection/transaction/query. If there is more than 1 query in transactions, execution time of all queries will be summarized. The same rule is for connection time calculation.</td>
</tr>
<tr>
<td>Prepare Time</td>
<td></td>
</tr>
<tr>
<td>Execute Time</td>
<td></td>
</tr>
<tr>
<td>Fetch Count</td>
<td>Applicable only for statements. Number of rows, as it's reported by fbclient.dll</td>
</tr>
<tr>
<td>Protocol</td>
<td>Firebird protocol version for current session.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of fbclient.dll/gds32.dll. Version detection is not 100% correct: minor versions are considered as the same, JayBird and .NET Provider are considered as the same, InterBase 8.x = InterBase 9.x</td>
</tr>
</tbody>
</table>

In the following table you can see details for the values appeared in the first column in FBScanner Viewer for SQL statements rows:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Allocated. Initial phase of SQL query life cycle</td>
</tr>
<tr>
<td>P</td>
<td>Prepared. Indicates that statement was prepared</td>
</tr>
<tr>
<td>E</td>
<td>Execute. Query is being executing at the moment</td>
</tr>
</tbody>
</table>
## Tags

Tags allow assigning readable identifiers (names) to Connections, Queries and Transactions. You just need to add these commentaries:

```sql
SELECT COUNT(*) FROM RDB$DATABASE
/* FBSCANNER$CON_NAME=My_application;
   FBSCANNER$TR_NAME=Read_only_transaction_N1;
   FBSCANNER$ST_NAME=Customers_list_query; */
```

- **FBSCANNER$CON_NAME=** sets the name of connection. After the first assignment this name will be kept during the whole connection life.

- **FBSCANNER$TR_NAME=** sets the name of transaction. After the first assignment this name will be used during the whole life of transaction.

- **FBSCANNER$ST_NAME=** sets the name of query.

Tags are showed in the first column in FBScanner Viewer grid, and it’s possible to filter tags by their names.

Tags are useful to quickly answer the following frequent questions:

- What program has launched this query? (developers need to mark with FBSCANNER$CON_NAME tag each database connection)

- What is the transaction for this query? (developers need to use FBSCANNER$TR_NAME tag to mark transactions)

- What is this very long query? (developer can mark long queries with readable names like “Annual report”).

## FBScanner Viewer Menu

FBScanner Viewer offers wide range of options to make debugging and optimization easier, which are accessible through its menu:

- **Server**
  - Connect To
Monitoring

- Disconnect To
- Recent Servers
- Exit

**Connections**
- Disconnect
- Disconnect Clients…
- Kill Process
- Latest Queries
- Oldest Connection
- Process Priority…
- Ping Client
- Ping All Clients
- Extract Plans

**Transactions**
- OAT

**Tools**
- **View Style**
  - Database Administrator (connections only)
  - Database Developer (without transactions)
  - Database Developer (with transactions)
- Language — English, Italian, Russian, Portuguese
- Plugins
- Options

**Columns** — list of columns

**Help**

**Server**

To connect to the FBScanner Service select Service\Connect To. The following dialog will appear:
After selecting the server FBScanner Viewer will ask for password. There are 2 passwords — for read-only access and for administrator (full) access. By default the password for read-only access is blank.

**Tip**
To setup passwords for FBScanner Viewer access you need to go to “FBScanner Configuration” — “Advanced Settings”.

**Server|Disconnect** disconnects FBScanner Viewer from FBScanner Service.

**Server|Recent Servers** shows list of most recent FBScanner Services where FBScanner Viewer connected to.

**Exit** closes FBScanner Viewer.

**Connections**

“Disconnect”, “Disconnect clients” and “Kill Process” menu options are available only when connected to FBScanner Service with administrative rights.

**Disconnect** will ask to close the current connection (highlighted in the main FBScanner Viewer grid):
“Disconnect clients” runs the following dialog:

In the right side there is a list of connections, represented by databases names, or clients, or user, according the filter above.

Using > and < buttons, administrator can select connections to be disconnected and then click “Disconnect” button.

Disconnect will be done by emulation of 10054 error — there will be appropriate record(s) in the firebird.log (interbase.log) and in FBScanner.log.

Kill

There are few cases when you need to kill Firebird process, and we do not recommend it.

“Kill process…” asks for explicit killing of Firebird process, and it works only at local FBScanner and Classic Architecture:
It will not work with SuperServer or SuperClassic architectures.

“Latest Queries” shows list of 20 most recent queries in the selected connection:

It's useful for ad-hoc debugging, it works like “Rewind” button.

Tip
For full-fledged logging of SQL traffic enable SQL logging feature in FBScanner Service, and use FBScanner LogAnalyzer to look through the log.

“Oldest Connection” shows the oldest connection in the grid.

“Process Priority” is applicable only for local FBScanner installation with Classic architecture. It enables to set process priority for Classic instances.

“Ping Client” allows to check – is selected connection still alive?

“Ping All Clients” checks all connections in the same way.

“Extract plans” starts plan extracting for selected connect. Extracted plans are shown in the grid, and also stored in the SQL (or text) log. If logging is not enabled, nothing happens. To enable plan extraction for all connects, use appropriate setting in “FBScanner Configuration”.

Transactions
The single option Transactions\OAT will put selection in the grid to the oldest active transaction.
Tools

In menu “Tools” we can see several options. With “View Style” user can select the most suitable representation of grid data:

- Database Administrator (connections only)
- Database Developer (without transactions)
- Database Developer (with transactions)

FBScanner Viewer is localized in 4 languages. Use Tools\Language to switch between languages:

“Plugins” option enables plugins. For more information please contact support@ib-aid.com

“Options” is another way to change some of FBScanner Service parameters.
Please consider appropriate session of this guide for details of FBScanner Service Configuration.

**SQL log structure**

FBScanner stores SQL traffic in the following table:

```sql
CREATE TABLE FBSCANNER$LOG
(
    ID BIGINT NOT NULL,
    IDATTACHMENT BIGINT,
    IDTRANSACTION BIGINT,
    PID INTEGER,
    ROW_TYPE INTEGER NOT NULL,
    CLIENT_IP VARCHAR(24),
    CLIENT_NAME VARCHAR(256),
    CUSTOM_NAME VARCHAR(256),
    SUBNET_NAME VARCHAR(256),
    DB_FILENAME VARCHAR(512),
    DB_USER VARCHAR(512),
    DB_ROLE VARCHAR(512),
    START_TIME TIMESTAMP DEFAULT 'NOW' NOT NULL,
    END_TIME TIMESTAMP,
    LAST_ACTIVITY TIMESTAMP DEFAULT 'NOW' NOT NULL,
    LAST_RETAINING TIMESTAMP,
    WORK_TIME INTEGER DEFAULT 0 NOT NULL,
    CPU_TIME_USER INTEGER DEFAULT 0 NOT NULL,
    CPU_TIME_PRIVILEGED INTEGER DEFAULT 0 NOT NULL,
    FETCH_COUNT INTEGER DEFAULT 0 NOT NULL,
    RESULT INTEGER,
    SQL_TEXT BLOB SUB_TYPE 1 SEGMENT SIZE 80,
    SQL_TEXT2 BLOB SUB_TYPE 1 SEGMENT SIZE 80,
    SQL_PLAN BLOB SUB_TYPE 1 SEGMENT SIZE 80,
    PREPARE_TIME INTEGER DEFAULT 0 NOT NULL,
    EXECUTE_TIME INTEGER DEFAULT 0 NOT NULL
);
```

**Logical structure**

There are 3 levels of hierarchy in this table:

- **ID** — primary key
- **IDATTACHMENT** and **IDTRANSACTION** — foreign keys referenced to FBSCANNER$LOG.ID
- **ROW_TYPE** — hierarchy level (0, 1, 2)

**Table 4.1. Level 1. Connection.ROW_TYPE = 0**

<table>
<thead>
<tr>
<th>PID</th>
<th>Process ID (only for local FBScanner)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROW_TYPE</td>
<td>0</td>
</tr>
<tr>
<td>CLIENT_IP</td>
<td>IP address of client</td>
</tr>
<tr>
<td>CLIENT_NAME</td>
<td>DNS name</td>
</tr>
<tr>
<td>CUSTOM_NAME</td>
<td>Connection tag (if assigned in query text)</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>SUBNET_NAME</td>
<td>Logical name of subnet. See file FBScanner.subnets</td>
</tr>
<tr>
<td>DB_FILENAME</td>
<td>Database alias or full database path</td>
</tr>
<tr>
<td>DB_USER</td>
<td>User name</td>
</tr>
<tr>
<td>DB_ROLE</td>
<td>User role</td>
</tr>
<tr>
<td>START_TIME</td>
<td>Start of connection</td>
</tr>
<tr>
<td>END_TIME</td>
<td>End of connection</td>
</tr>
</tbody>
</table>

**Table 4.2. Level 2. Connection.ROW_TYPE = 1**

<table>
<thead>
<tr>
<th>IDATTACHMENT</th>
<th>Connection ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROW_TYPE</td>
<td>1</td>
</tr>
<tr>
<td>CUSTOM_NAME</td>
<td>Transaction tag (if assigned)</td>
</tr>
<tr>
<td>START_TIME</td>
<td>Transaction start time</td>
</tr>
<tr>
<td>END_TIME</td>
<td>Transaction end time</td>
</tr>
<tr>
<td>LAST_RETAINING</td>
<td>Time of most recent commit retaining or rollback retaining</td>
</tr>
<tr>
<td>RESULT</td>
<td>0 – transaction is active</td>
</tr>
<tr>
<td></td>
<td>1 – Commit</td>
</tr>
<tr>
<td></td>
<td>2 – Rollback</td>
</tr>
<tr>
<td>SQL_TEXT</td>
<td>Transaction flags</td>
</tr>
</tbody>
</table>

**Table 4.3. Level 2. Connection.ROW_TYPE = 2**

<table>
<thead>
<tr>
<th>IDATTACHMENT</th>
<th>Connection ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDTRANSACTION</td>
<td>Transaction ID</td>
</tr>
<tr>
<td>ROW_TYPE</td>
<td>2</td>
</tr>
<tr>
<td>CUSTOM_NAME</td>
<td>Query tag (if assigned)</td>
</tr>
<tr>
<td>START_TIME</td>
<td>Query start time</td>
</tr>
<tr>
<td>WORK_TIME</td>
<td>Time till the answer from server</td>
</tr>
<tr>
<td>CPU_TIME_USER</td>
<td>CPU Time (local only)</td>
</tr>
<tr>
<td>CPU_TIME_PRIVILEGED</td>
<td>CPU Kernel Time (local only)</td>
</tr>
<tr>
<td>FETCH_COUNT</td>
<td>Number of records, returned by query</td>
</tr>
<tr>
<td>RESULT</td>
<td>0 – query executed successfully, otherwise this field contains SQLCODE of error</td>
</tr>
<tr>
<td>SQL_TEXT</td>
<td>Query text (with parameters)</td>
</tr>
</tbody>
</table>
Indices in the log

Initially log database contains only primary key index. FBScanner Log Analyzer creates necessary indices at the first connect.

FBScanner Feature Matrix

<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>FBScanner mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td>Operation Systems Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Linux, Mac OS X, Free BSD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firebird and InterBase versions supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firebird 1.0, Yaffil 1.0 (including logging)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Firebird 1.5 (including logging)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Firebird 2.0 (including logging)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Firebird 2.1 (including logging)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Firebird 2.5 (including logging + SuperClassic support)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>InterBase 6.0-2009/XE (including logging)</td>
<td>X</td>
</tr>
</tbody>
</table>

Connections

1. **Information about established connections in the FBScanner Viewer:**

   - Firebird/InterBase user login | X | X
   - IP-address or computer name   | X | X
   - Connection time and time of the latest activity | X | X
   - Priority of processes (only for Classic architecture) | X

1.2 **Connection management (requires logging to FBScanner Viewer with Admin rights):**

   - Safe disconnect of one or several connections using TCP/IP connection interruption (imitation of 10054 error) | X | X

147
<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>FBScanner mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Changing of processes priority in Classic architecture (for example, to adjust priority of long running report or something like this. Using tags administrator can recognize connection where report is working — see below in “Tags”).</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Automatic priority settings for Firebird with Classic architecture. In FBScanner configuration administrator can set up automatic correspondence:</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Specified IP or subnet of IPs – set priority X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specified hostname – set priority X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specified database name – set priority X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specified user login name – set priority X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Killing of Classic processes, not recommended to use, but sometimes it is helpful</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Ability to restrict all connections (to perform some operations which require exclusive access)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Filtering connections viewing using all connections parameters (except time information)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>White and black list of databases to connect</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>White and black list of IP addresses (clients)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Restriction of connections # — administrator can limit the number of connections</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Emulation of “Wrong login/password” error for denied connections</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Detection of old/incorrect versions of fbclient.dll/gds32.dll</td>
<td>X</td>
</tr>
<tr>
<td>1.3</td>
<td><strong>Logging events related with connections</strong></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>FBScanner logs unsuccessful login attempts in the FBScanner.log. For each unsuccessful login attempt FBScanner writes the following information: IP-address, login name, database and time of login attempt.</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>If connection was broken (10054 error), FBScanner determines and logs one of the 5 type of disconnects:</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Client application was closed improperly (for instance, application was closed by Task Manager)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection was closed by time-out (it’s possible to set forced disconnect in FBScanner to close connect by time-out too)</td>
<td></td>
</tr>
</tbody>
</table>
## Monitoring

<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>FBSscanner mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td>Server crashed (fbserver or fb_inet_server crashed)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server process (fbserver or fb_inet_server) was killed from the FBSscanner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disconnect of connections from FBSscanner Viewer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For all cases above FBSscanner writes the IP-address of disconnected client(s) and the reason of disconnect. This is very useful feature to find and eliminate 10054 errors.</td>
<td></td>
</tr>
</tbody>
</table>

### 2. Transactions

#### 2.1. Transactions are shown inside appropriate connections

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions' flags</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifetime of transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using OAT button you can find the oldest active transaction in real-time and review related connection/queries.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3. Queries (statements)

#### 3.1 Information about queries (statements)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Query text</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction of the query</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status (prepare/execute/...)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filtering by statement status (by default Closed statements are hidden)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant CPU load indicator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If query PREPARE or execution caused error, FBSscanner writes SQLCODE to the log (for example, primary key violation)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 3.2 Additional operations with queries

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-hoc plan extraction for queries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can be performed for all connections (should be set ON in FBSscanner configuration utility)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can be turned ON/OFF for selected connection only in the FBSscanner Viewer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>In both cases plans will be logged to the overall log if logging is ON.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4. Tags
# Feature

Tags allow assigning readable identifiers (names) to Connections, Queries and Transactions. You just need to add these commentaries:

```sql
SELECT COUNT(*) FROM RDB$DATABASE /* FBSCANNER$CON_NAME=My_application;
FBSCANNER$TR_NAME=Read_only_transaction_N1;
FBSCANNER$ST_NAME=Customers_list_query; */
```

- **FBSCANNER$CON_NAME** = sets the name of connection. After the first assignment this name will be kept during the whole connection life.
- **FBSCANNER$TR_NAME** = sets the name of transaction. After the first assignment this name will be used during the whole life of transaction.
- **FBSCANNER$ST_NAME** = sets the name of query.

Tags are showed in special column in FBScanner Viewer

It's possible to filter tags by their names

Tags are useful to quickly answer the following frequent questions:

What program has launched this query? (developers need to mark with FBSCANNER$CON_NAME tag each database connection)

What is the transaction for this query? (developers need to use FBSCANNER$TR_NAME tag to mark transactions)

What is this very long query? (developer can mark long queries with readable names like “Annual report”)

### 5. Logging

Logging allows intercepting all queries and writing them to the external Firebird database. FYI, logging cannot be replaced with Firebird 2.1 or InterBase system tables, because they provide only snapshots of programs.

- Connections, queries and transactions are logged
- All executed queries are logged (only prepared quires skipped)
- Queries are stored with information about their connection and transaction
<table>
<thead>
<tr>
<th>#</th>
<th>Feature</th>
<th>FBScanner mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Agent</td>
</tr>
<tr>
<td></td>
<td>All transactions are logged, even rolled back. Transaction log</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>record has column RESULT which shows was transaction committed or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rolled back.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If plan extraction is on, queries plans are logged too</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Automatic creation of database for logging</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Automatic creation of tables to logging in any Firebird database</td>
<td>X</td>
</tr>
</tbody>
</table>
Database structure analysis

5.1. Overview of Firebird database structure

The first thing we have to say about the structure of Firebird database is that it represents a set of pages of strictly defined size: 4096, 8192, 16384 (previous versions of Firebird supported page sizes 1024 and 2048).

Pages can be of different types, each of which serves its certain purpose.

Pages of the same type don't go strictly one by one — they can be easily mixed, allocated in file in the order they were created by server when extending or creating databases.

### Table 5.1. Page types

<table>
<thead>
<tr>
<th>Page Type</th>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pag_undefined</td>
<td>0</td>
<td>Undefined – If a page has this page type, it is most likely empty</td>
</tr>
<tr>
<td>pag_header</td>
<td>1</td>
<td>Database header page</td>
</tr>
<tr>
<td>pag_pages</td>
<td>2</td>
<td>Page inventory page (or Space inventory page – SIP)</td>
</tr>
</tbody>
</table>
## 5.2. How to analyze database structure with HQbird Database Analyst (IBAnalyst)

**IBAnalyst** is a tool that assists a user to analyze in detail Firebird database statistics and identify possible problems with database performance, maintenance and how an application interacts with the database. IBAnalyst graphically displays Firebird database statistics in a user-friendly way and highlights the following problems:

- tables and BLOBs fragmentation,
- record versioning,
- garbage collection,
- indices effectiveness, etc

Moreover, IBAnalyst can automatically make intelligent suggestions about improving database performance and database maintenance.

IBAnalyst can get statistics from the live production databases through Services API (recommended), or analyze text output of `gstat -a -r ...` commands. Statistics from the peak load periods can give a lot of information about actual performance problems in production databases.

Main features of IBAnalyst are listed below:

- Retrieving database statistics via Service API and from gstat output.
- Summary of all actual and possible problems in database
- Colored grid representation of tables, indices and table->indices, which highlights fragmented tables, poor indices and so on.
- Automatic expertise of database statistics provides recommendations and “how-to” for the following things:
  - Optimal database page size
Database structure analysis

• Transactions state and gap between critical transactions
• Different database flags
• Index Depth
• Index Key Duplicates
• Fragmented Tables
• Record Versions
• Very Big Tables
• and more…

How to get statistics from Firebird database in right way

Right time, right place

It sounds strange, but just taking statistics via gstat or Services API is not enough. Statistics must be taken at the right moment to show how applications affect data and transactions in database. Worst time to take statistics is

Right after restore

After backup (gbak -b db.gdb) without –g switch is made

After manual sweep (gfix –sweep)

It is also correct that during work there can be moments where database is in correct state, for example, when applications make less database load than usual (users at launch, dinner or its by specific business process times).

How to catch when there is something wrong in database?

Yes, your applications can be designed so perfect that they will always work with transactions and data correctly, not making sweep gaps, lot of active transactions, long running snapshots and so on. Usually it does not happen. At least because some developers test their applications running 2-3 simultaneous users at the same time, not more. Thus, when they set up written applications for 15 and more simultaneous users, database can behave unpredictably. Of course, multi-user mode can work Ok, because most of multi-user conflicts can be tested with 2-3 concurrently running applications. But, next, when more concurrent applications will run, garbage collection problems can come (at least). And this can be caught if you take statistics at the correct moments.

If you does not experience periodical performance problems

This can happen when your applications are designed correctly, there is low database load, or your hardware is modern and very powerful (enough to handle well current user count and data).

The most valuable information is transactions load and version accumulation. This can be seen only if you setup regular statistics saving.
Database structure analysis

The best setup is to get hourly transaction statistics. This can be done by running

```
gstat -h db.gdb>db_stat_<time>.txt
```

where

- `db.gdb` is your database name,
- `db_stat_<time>.txt` is text file where statistics will be saved,
- `<time>` — current date and time when statistics was taken.

Also you can schedule to gather database statistics with HQbird FBDataGuard, job "Database: Statistics".

If you experience periodical performance problems

These problems usually caused by automatic sweep run. First you need to determine time period between such a performance hits. Next, divide this interval minimally to 4 (8, 16 and so on). Now information systems have lot of concurrent users, and most of performance problems with not configured server and database happens 2 or 3 timers per day.

For example, if performance problem happens each 3 hours, you need to take

```
gstat -h db.gdb
```

statistics each 30-45 minutes, and

```
gstat -a -r db.gdb -user SYSDBA -pass masterkey
```

each 1-1.5 hour. The best is when you take `gstat -a -r` statistics right before forthcoming performance hit. It will show where real garbage is and how many obsolete record versions accumulated.

What to do with this statistics

If your application explicitly uses transactions and uses them well, i.e. you know what is read

```read_committed```

and when to use it, your snapshot transactions lasts no longer than needed, and transactions are being active minimal duration of time, you can tune sweep interval or set it off, and then only care about how many updates application(s) makes and what tables need to be less updated or cared about updates.

What does this mean, you can ask? We'll give example of some system, where performance problems happened each morning for 20-30 minutes. That was very sufficient for morning applications, and could not last longer.

Database admin was asked correct questions, and here is the picture:

Daily work was divided by sections — analytic works in the morning, than data is inserted and edited by usual operators, and at the end of the day special procedures started gathering data, that would be used for analytic next day (at least).
The last work on database at the end of day was lot of updates, and updates of those tables which analytic used in the morning. So, there were a lot of garbage versions, which started to be collected by application, running in the morning.

And, the answer to that problem was found simple — to run `gfix -sweep` at the end of the day.

Sweep reads all tables in database and tries to collect all garbage versions for committed and rolled back transactions. After sweeping database became clear nearly it comes after restore.

And, "morning problem" has gone.

So, you need to understand statistics with lot of other factors:

- how many concurrent users (average) work during the day
- how long is the working day (8, 12, 16, 24 hours)
- what kind of applications running at different day times, and how they affect data being used by other applications, running at the same time or next. I.e. you must understand business processes happening during the whole day and whole week.

**When DBA can't do nothing**

Sadly to say, these situations happen. And again, example:

Some system installed for ~15 users. Periodically performance is so bad, that DBA needs to restart server. After server restart everything works fine for some time, then performance gets bad again. Statistics showed that average daily transactions is about 75,000, and there are active transactions running from the start of day to the moment when performance getting down.

Unfortunately, applications were written with BDE and with no transactions using at all; i.e. all transaction handling was automatic and used by BDE itself. This caused some transactions to stay active for a long time, and garbage (record versions) accumulated until DBA restarted server. After restart the automatic sweep will start, and the garbage will be collected (eliminated).

All these was caused by applications, because they were tested only with 2-3 concurrent users, and when they became ~15, applications started to make very high load.

Need to say that in that configuration 70% of users were only reading data, and other 30% were inserting and updating some (!) data.

In this situation the only thing that can make performance better is to redesign transaction management in this application.

**How IBAnalyst can help find problems in your Firebird database**

Let's walk through the key features of IBAnalyst. When you look at your database statistics in IBAnalyst first time, things can be not clear, especially if IBAnalyst shows lot of warnings by colored red and yellow cells at Summary, Tables and Index views. Let's consider several real statistics examples.

**Summary View**

Summary contains the most important information extracted from database statistics. Usually full statistics of database contains hundreds of Kbytes and it is not easy to recognize the important information.
Below is the description of database objects and parameters that you may see in Summary. For description of visible problems (marked red or yellow) see column hints or Recommendations output.

<table>
<thead>
<tr>
<th>Object or parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database name</strong></td>
<td>Name of analyzed database.</td>
</tr>
<tr>
<td><strong>Creation date</strong></td>
<td>Database creation date. When it was created by CREATE DATABASE statement or restore (gbak -c/-r).</td>
</tr>
<tr>
<td><strong>Statistics date</strong></td>
<td>When statistics was taken — statistics file date or Services API call date (now).</td>
</tr>
<tr>
<td><strong>Page size</strong></td>
<td>Page size is the physical parameter of database. The best page size is 4096 or 8192 bytes. Other page sizes (less than 4096) marked as red. For better performance restore database from backup using 4K or 8K page size. (Note: Firebird 2.0+ can use 16K page size).</td>
</tr>
<tr>
<td><strong>Forced Write</strong></td>
<td>It shows the mode of changed pages writing: synchronized or asynchronized — appropriate setting is ON or OFF. OFF is not recommended, because server crush, power failure or other problems can cause database corruption.</td>
</tr>
<tr>
<td><strong>Dialect</strong></td>
<td>Current database dialect.</td>
</tr>
<tr>
<td><strong>Sweep interval</strong></td>
<td>Current sweep interval value. Marked yellow if it is not 0, and marked red if Sweep Gap greater than Sweep interval.</td>
</tr>
<tr>
<td><strong>On Disk Structure</strong></td>
<td>ODS. It is a database physical format. See hint to know ODS number for particular IB/FB versions</td>
</tr>
<tr>
<td><strong>Transaction block</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Oldest transaction</strong></td>
<td>Oldest interesting transaction. The oldest transaction id that was rolled back, or in limbo.</td>
</tr>
<tr>
<td><strong>Oldest snapshot</strong></td>
<td>Oldest snapshot transaction Id of transaction that was oldest active when currently oldest snapshot started.</td>
</tr>
<tr>
<td><strong>Oldest active</strong></td>
<td>Oldest active transaction Id of oldest still active transaction.</td>
</tr>
<tr>
<td><strong>Next transaction</strong></td>
<td>Newest available transaction id</td>
</tr>
<tr>
<td><strong>Sweep gap (snapshot − oldest)</strong></td>
<td>For ODS 10.x databases. Difference between Oldest Snapshot and Oldest Interesting transaction. If it is greater than sweep interval, and sweep interval is &gt; 0, Firebird tries to run sweep, and it can slowdown performance.</td>
</tr>
<tr>
<td><strong>Snapshot gap (active − oldest)</strong></td>
<td>Difference between Oldest Active and Oldest transaction. Same as previous sweep gap.</td>
</tr>
<tr>
<td><strong>TIP size</strong></td>
<td>Transaction Inventory Page size, in pages and kilobytes. TIP holds transaction state for every transaction was started from database</td>
</tr>
</tbody>
</table>
Database structure analysis

<table>
<thead>
<tr>
<th>Object or parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>creation (or restore). It is computed as Next transaction div 4 (bytes).</td>
<td></td>
</tr>
<tr>
<td><strong>Snapshot TIP Size</strong></td>
<td>Size of Transaction Inventory Pages that needed for snapshot transactions. Indicates how much memory will take each snapshot transaction to check concurrent transactions state.</td>
</tr>
<tr>
<td><strong>Active transactions</strong></td>
<td>Currently active (on the moment when statistics was taken from database) transaction count (Next – Oldest Active). Maybe incorrect, because it can be one active transaction and lot of ahead transactions committed. Anyway, active transactions prevent garbage collection.</td>
</tr>
<tr>
<td><strong>Transactions per day</strong></td>
<td>Simply divides Next transaction by days’ count between database creation date and date statistics taken. Shows average transaction per day, and useless if it is not production database. Transaction warnings mostly based on average transactions per day count.</td>
</tr>
<tr>
<td><strong>Data versions percent</strong></td>
<td>Percent of record versions in database. Also total records size and versions size for all tables is shown, and total index size. Row is not shown when statistics does not contain record count information (gstat -a without -r option). Note that there can be lot of other data (transaction inventory pages, empty pages and so on) in your database.</td>
</tr>
</tbody>
</table>

**Table/Index lists** (also reported in recommendations)

| **Fragmented Tables**            | Here you can view tables (with data > 200 kilobytes) that have average fill less than 60% (File/Options/Table average fill).                                                                                                                                                                                                                                                                                                                                                   |
| **Versioned Tables**             | List of tables that have Versions greater than Records, set in Options/Tables.                                                                                                                                                                                                                                                                                                                                                                                                       |
| **Tables fragmented with blobs**  | List of tables that have blob fields with data size less than database page size.                                                                                                                                                                                                                                                                                                                                                                                                     |
| **Massive deletes/updates**      | List of tables that had lot of data deleted/updated by one delete/update statement.                                                                                                                                                                                                                                                                                                                                                                                                         |
| **Very big tables**              | Tables that are close to technical InterBase limit (36 gigabytes per table). You will see warning beforehand problem can occur.                                                                                                                                                                                                                                                                                                                                         |
| **Deep Indices**                 | Indices with depth more than 3 (Options/Index)                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| **Bad Indices**                  | Indices with big MaxDup and TotalDup values                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| **Broken or incomplete indices** | Indices with key count less than record count. This can happen when index is broken or when statistics is taken during index creation or re-activation.                                                                                                                                                                                                                                                                                                                                 |
| **Useless Indices**              | Indices with Unique column = 1. May be deleted or deactivated, because they are useless for index search or sort operations.                                                                                                                                                                                                                                                                                                                                                 |
| **Tables with no records**       | List of tables with Records = 0. This can be by design (temporary tables), or they can be just forgotten by database developer.                                                                                                                                                                                                                                                                                                                                                 |
Summary page shows a lot of information, but the most valuable is transactions state (please read description of possible transactions states in IBAnalyst help, it is available by clicking F1 or in menu Help).

At this screenshot you can see that some transaction is active for a long time, “60% of daily average”. IBAnalyst marks such transaction's state by red, because this transaction may prevent accumulated versions to be considered as garbage by server, and so, to be garbage collected. This is a possible reason of slowness: the more versions exist for some record, the more time it will takes to read it.

In order to find this long-running transaction you can use MON$Logger module of FBScanner, or perform direct query of MON$ tables. Then, to find out which tables were affected by long running transactions (tables with a lot of record versions) you need to go to “Tables” view of IBAnalyst.

**Tables view**

View Tables contains the information about all database tables. It represents important statistical information about each table. All table warnings are marked (see details below).

You can see the following columns (Columns Records, RecLength, VerLen, Versions, Max Vers are visible only if statistics was generated with `gstat -r` or with “Include record/rec versions” checkbox enabled):
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records</td>
<td>Record count. Marked pink if table fragmented by blob fields which data is less than database page size. Hint shows real table fragmentation and average records if there were no blob fields. Such fragmentation can cause bad performance for big table joins or natural scans.</td>
</tr>
<tr>
<td>RecLength</td>
<td>Average record length. Depends on record data, especially on char/varchar columns data. Min physical record length is 17 bytes (record header + all fields are null), max – as declared in table. Statistics show this data without record header count, in this case RecLength can be 0 (if nearly all records are deleted)</td>
</tr>
<tr>
<td>VerLen</td>
<td>Average record version length. If it is close to RecLength, almost all record is being updated. If VerLen is 40-80% and not greater of RecLength, then Versions are mostly updates. If VerLen greater than 80-90% of RecLength, then maybe Versions are mostly deletes, or update is made by char/varchar columns with new, greater data. Marked yellow if it's size is greater than specified % (Options/Record/Version size) of average record size.</td>
</tr>
<tr>
<td>Versions</td>
<td>Current record version count. More versions slowdown table reads. Also lot of versions means that there is no garbage collection performed or records are not read by anyone. Marked red if version count is greater than Records. (Options/Record Versions).</td>
</tr>
<tr>
<td>Max Vers</td>
<td>Max record versions for one particular record. Marked blue when it is equal to 1 and Versions is non-zero. It means that there were massive update/delete operation. See Options, Table, Massive deletes updates option.</td>
</tr>
<tr>
<td>Data Pages</td>
<td>Allocated data pages</td>
</tr>
<tr>
<td>Size, Mb</td>
<td>DataPages * Page Size, in megabytes. I.e. this is total table size, records + versions. Graph shows percentage of that table from the whole data size.</td>
</tr>
<tr>
<td>Idx Size, Mb</td>
<td>Sum of all indices size for that table. Graph shows percentage of that value to total size of all indices.</td>
</tr>
<tr>
<td>Slots</td>
<td>Count of links to data pages. Empty links are Slots-Data Pages. Doesn't affect disk space or performance.</td>
</tr>
<tr>
<td>Average Fill</td>
<td>Average data page fill %. Can be computed as (DataPages * Page Size) / Records * RecLength. Low page fill means that table is &quot;fragmented&quot;. Frequent updates/deletes can fragment data pages. Marked red if average fill rate is less than 60% (go to Options/Average Fill to adjust it). Marked yellow if it is an artifact of high table fragmentation when it's record is too small (11-13 bytes).</td>
</tr>
<tr>
<td>Real Fill</td>
<td>Because we found that Average Fill, calculated by gstat, sometimes gives wrong results (at least for tables with small blobs), we placed here calculated column, that counts average</td>
</tr>
</tbody>
</table>
Database structure analysis

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fill not by data pages, but by records+versions, including record header.</td>
<td>Shows page count having corresponding fill rate. Can be turned on/off in Options dialog</td>
</tr>
<tr>
<td>20%, 40%, 60% and 100% fill</td>
<td>How big is that table plus it's indices in %, related to other tables.</td>
</tr>
</tbody>
</table>

At “Tables” view you can see tables and their important parameters: number of records, number of record versions, record length, maximum number of versions, etc.

You can sort this view to find the largest tables. Especially we are interested tables with many record versions – many record versions will make garbage collection for affected tables longer. Usually it is necessary to change update and delete algorithms to get rid of many record versions.

Row Versions show total versions count for particular table, and row Max Vers shows maximum versions reached by some record. For example, if you look at table SITE, there are 40611 records, total versions are 76142, but one record has 501 versions. Reading and parsing such packet from disk takes more time, so, reading this record is slower than reading others.

This picture also shows a lot of tables where data was deleted. But, because of long running transaction, server can't delete these versions, and they still on disk, still indexed, and still being read by server when reading data.

**Index view**

View **Indices** represents all indices in your database. You can estimate the effectiveness of indices with the following parameters (problem indices are marked red — see smart hints for details)
## Database structure analysis

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Depth</strong></td>
<td>Index depth is the page count that engine reads from disk to walk from index root to record pointer. Optimal index depth is 3 or less. When Depth is 4 and higher, it is recommended to increase database page size (backup, then restore with -page_size option). This column will be marked red if index depth is greater than 3 (Options/Index/Index Depth). More chances to exceed optimal depth have indices built on long char/varchar columns.</td>
</tr>
<tr>
<td><strong>Keys</strong></td>
<td>Index key count. Usually equals to Records. If Keys is bigger than Records and Versions count is greater than 0 it means that concrete field value was changed in those record versions. If Table.RecVersions is bigger than Keys, than this index field(s) are not changed during updates.</td>
</tr>
<tr>
<td><strong>KeyLen</strong></td>
<td>Average index key length. The less KeyLen, the more equal or similar (postfix) values (keys) stored in index.</td>
</tr>
<tr>
<td><strong>Max Dup</strong></td>
<td>Maximum duplicates count for particular key value. Some old gstat versions show no more than 32767 or 65535 — this bug is fixed in latest Firebird versions. Marked red if duplicates count is 30% of all keys. (Options/Index/Lot of key duplicates).</td>
</tr>
<tr>
<td><strong>Total Dup</strong></td>
<td>The overall count of keys with the same values. Some old gstat versions show no more than 32767 or 65535 — this bug is fixed in latest Firebird versions. The closer this value to Keys count, the less effective will be searching using this index, especially when search is made using more than one index. Total Dup value can be counted as Keys minus unique keys count (index statistics is nonlinear). Marked yellow if $1/(\text{Keys} - \text{TotalDup})$ greater than 0.01, and red if in addition MaxDup is marked red too. This constant (0.01) is used by optimizer (see sources in opt.c/opt.cpp) as usable index selectivity border. Optimizer will still use that index if none other index with better selectivity exists for some condition.</td>
</tr>
<tr>
<td><strong>Uniques</strong></td>
<td>Count of different key values. Primary and unique key indices will show same value as in Keys column. Useful to understand how many different values stored in index — is it useful or not. Index is useless if Unique column shows 1 (marked yellow).</td>
</tr>
<tr>
<td><strong>Selectivity</strong></td>
<td>Information from rdb$indises.rdb$statistics, only visible if “load table/index metadata” was On. If selectivity stored in database differs from computed selectivity, yellow warning shown (less than 20% difference) or red (higher than 20% difference). Blue warning is shown when index is empty but it's selectivity is not 0. Selectivity of inactive indices are ignored.</td>
</tr>
<tr>
<td><strong>Size, Mb</strong></td>
<td>Index size in megabytes. Gap show percentage of that index size related to total size of all indices.</td>
</tr>
<tr>
<td><strong>Average Fill</strong></td>
<td>Average index pages fill rate, in %. Marked red if average fill rate is less than 50% (go to Options/Average Index Fill to adjust</td>
</tr>
</tbody>
</table>
### Database structure analysis

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>it)</td>
<td>Fragmented index results more page reads as usual, and it's Depth can be higher. Can be fixed by alter index inactive/active, if it is not index created by primary, unique or foreign key constraints.</td>
</tr>
<tr>
<td>Leaves</td>
<td>Leaf page count (pages with keys and record pointers).</td>
</tr>
<tr>
<td>20%, 40%, 60% and 100% fill</td>
<td>Shows page count having corresponding fill rate. Can be turned on/off in Options dialog</td>
</tr>
</tbody>
</table>

Some production databases can have indices with the only key value indexed. This can happen because database was developed “to be extended in the future”, or, someone just experimented with the indices during development or tests. You can see these indices as “Useless” in IBAnalyst:

- I_NUMBER, etc, built on the column that has only one value for all rows. These indices are really useless, because

- Optimizer may use this index if you specify “where field =...”. Since field contains only one value, using index will cause useless reading of index pages from disk to memory, and consume memory (and time) when server will prepare which rows to show for that query.

- Creating indices is the part of restore process. Extra indices adds extra time.

Of course, that is not all that you can find about your database in IBAnalyst. You can also find

- average number of transactions per day
- was there rollbacks or lost connections, and when
- how big (in megabytes) each table and index
• tables that have records interchanged by blobs, and thus reading only records is slower
• empty tables — just forgotten, or empty at the time when statistics was taken
• indices with lot of duplicate keys (you can consider about column value distribution)
• indices with depth 4 and greater — maybe you need to increase page size to speed up
6.1. What is HQbird Enterprise?

HQbird Enterprise is the advanced distribution of Firebird for big databases with monitoring, optimization and administration tools, it also includes the plugin for native master-slave replication and various performance improvements.

Compatibility

HQbird Enterprise is 100% compatible with Firebird 2.5.5+ and Firebird 3.0 – no changes in ODS are needed. To switch to HQbird and back no backup/restore is required, just stop/start Firebird and replace binaries. The replication is possible between nodes with the same version, i.e., not possible between 3.0 and 2.5.

How the replication works

HQbird replication works on the logical level: it replicates DML statements (INSERT/UPDATE/DELETE, stored procedures, etc) and DDL (CREATE/ALTER TABLE, etc) changes; no additional triggers needed. The only requirement for the current version of replication is to have unique or primary keys for all tables that need to be replicated.

In order to use the replication, you need to install HQbird instead of Firebird, register it (with trial or with the full license) and configure replication. HQbird should be running on the master server and on all replica servers.

Below we will consider how to setup Firebird replication with HQbird Enterprise.

You can use HQbird on Windows and Linux, with Firebird 2.5 and 3.0, 32 bit and 64 bit.

6.2. Installation

Please install HQbird Enterprise from the supplied distributive. If you have other version of Firebird installed, uninstall it first.
HQbird Enterprise configuration: Native Firebird replication and Performance Enhancements

To enable replication you need to have working and registered (trial or full) copy of HQbird 2020 or higher on your master and replica servers.

Please refer to the section 2 of this guide for details of HQbird Server installation.

6.3. Asynchronous replication for Firebird

HQbird supports 2 types of replication: asynchronous and synchronous. In the case of an asynchronous replication, the master server stores committed changes from the master database to the files (replication segments), which can be consumed asynchronously by one or more replica servers.

How the asynchronous replication works:

- Changes on the master side are journaled into the replication log files
- Journal consists of multiple segments (files)
- Replication (archived) segments are transferred to the slave and applied to the replica in the background
- Replica can be created and recreated online (without master's stop)

Important things to consider:

- Practical delay between master and replica is configurable, can be set to 15-30 seconds (default is 90 seconds)
- Delay between master and replica can grow in case of heavy load (due to the delayed processing of replication segments)
- Replica can be switched to the master (i.e., normal) mode with 1 command

Asynchronous replication is the recommended choice for HQbird Enterprise:

- it provides stability and anti-corruption protection of Firebird database,
 HQbird Enterprise configuration: Native Firebird replication and Performance Enhancements

- it can be configured quickly and easily,
- it does not require downtime to setup,
- it has online re-initialization (in HQbird 2020 and higher),
- it is suitable for distributed environments (when the replica is located in the cloud or at the remote location).

The following steps will be required to setup the asynchronous replication:

1. Configure HQbird for replication at the master
2. Create a copy of master database file
3. Setup database for replication at the replica (slave) server

**Step 1: Configure HQbird for replication at the master**

To setup replication, open HQbird FBDataGuard: run modern browser (Chrome, Firefox, etc) and open this local URL: [http://127.0.0.1:8082](http://127.0.0.1:8082) (port if configurable in HQBird ini files)

Enter default name and password: **admin/strong password**. Register Firebird server, and the following picture will appear:

![HQbird FBDataGuard interface](image)

Check that you are actually connected to the correct Firebird version — in the upper left corner in “Active server” widget should be version “… Firebird 2.5 HQbird” or “… Firebird 3.0 HQbird”.

After that click “Add database” in the right bottom corner and configure nick name and path to the database which will be master:
Note

Please note that database should be registered with its explicit path, not with the alias — the replication will not work with the alias.

After the successful registration of the database click on the icon in the header of database to setup replication:

Asynchronous replication at master

Asynchronous replication writes all changes in the master database to the replication log: the set of files called “replication segments”. Replica server pulls these segments and inserts into the replica database.
Previously we have registered H:\dbwmaster.fdb, it is the asynchronous master database in this example. To configure the asynchronous replication on the master side: select replication role: “Master”, then “Asynchronous”, and click “Save”.

![Database replication configuration dialog](image)

**Figure 6.1. Replication setup dialog for asynchronous replication**

The only parameter you can change is “**Force flush committed data in, seconds**”, it specifies how often we should move committed data to the archived replication segments.

By default, it is set to 90 seconds.

There are several optional parameters which you can change if you open detailed dialog with button “more>>”:
Let's consider all parameters in this dialog — just to give you idea what they do, **no need to change them**:

- **"Log directory"** — folder where operational logs will be stored. It is a system folder, completely operated by Firebird. By default, **no need to change its default value** `${db.path}.ReplLog` (db.path is where the database is located).

- **"Log archive directory"** — folder, where archived logs will be stored. According the default value `${db.path}.LogArch`, HQbird will create folder `DatabaseName.LogArch` in the folder with the database, so there is **no need to change this parameter**.

- The third parameter ("Override log archive command") is optional, **leave it empty**.

**Note**

Please note that replication parameters are initialized at the first connection to the database. That's why you need restart Firebird service (or all connections in case of Classic) after the replication configuration — such restart ensures that replication will start properly.
In this case, the replication log segments will be written first to $\{db.path\}.ReplLog (db.path is where the database is located — in our example it will be H:\DBWMaster.fdb.ReplLog), and after reaching the maximum segment size, or commit, or another trigger, the default archive command will be started – it will copy archived replication segments to $\{db.path\}.LogArch (in our example it will be H:\DBWMaster.fdb.LogArch).

After replication’s start, you should be able to see replication segment files in the folder specified in “Log directory” immediately after any operation at master database:

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbwmaster.fdb.log-000</td>
<td>05.09.2016 17:02</td>
<td>LOG-000 File</td>
<td>1 KB</td>
</tr>
</tbody>
</table>

The operational segments are rotated by the engine, and once each segment is completed, it is copied to archive log. Default segment size is 16Mb. Please note — you don’t need to do anything with operational segments!

After the commit and/or specified timeout of committed data, you will see archived segments in the folder, specified by “Log archive directory”.

Archive replication log is essentially the chronologically ordered list of completed operational segments. These files should be imported by replica server into the replica database.

**Important!**

For Linux users — make sure that folder with the database is owned by firebird user. HQbird runs under “firebird” user in Linux, and the folder with the database must have permissions for “firebird” to create logs folder (chown firebird -R /your/database/folder).

**How to copy replication segments from master server to the replica server?**

There are 2 popular ways to copy archived segments from the master server to the replica server(s): through network share and using Cloud Backup on master and Cloud Backup Receiver on replica.

**Network share**

You can share the folder with archived segments as a network share. In this case, Firebird service should have enough rights to read, write and delete files on that network share. Normally Firebird and HQbird services are started under LocalSystem account, which do not have access to the network shares. Change it to some powerful account (like Domain Admin).

**Cloud Backup/Cloud Backup Receiver**

We recommend using HQbird FBDataGuard to send replication segments from the master server to the replica through FTP: it compresses, encrypts and uploads segments to the specified FTP server. On that server, another HQbird FBDataGuard unpacks segments and copies to the necessary folder for further consumption by the replica.

**Note**

Please read about CloudBackup job for more details how to setup transfer of archived segments between master and replica(s).
**Step 2: Create a copy of master database**

To start replication we need to create an initial copy of the database file, which will be used as a target for the replication process. Let's refer to such database file as “replica”.

Starting with HQbird 2018 R2, the replica will be created automatically in the folder which will you specify in the dialog after clicking on “Reinitialize replica database”.

If you have enough space in the folder with the database, just leave the path empty, and click Ok, and replica will be created near the database. Or, you can specify other destination on the local drives with enough free space.

**Important!**

If there will be not enough free space (less than 105% of the database size), HQbird will not create replica copy — there will be an appropriate error message.

If you click Ok, HQbird will start the process of replica creation. There will be an appropriate message about it:
In case of default action, the resulted database will be in the same folder with the database. The name of the replica will be DATABASE_NAME.EXT.DD-MMM-YYYY_NNNN.4replica — for example, employee30.fdb.17-Apr-2018_142507.4replica

**Note**

Please note — creating of replica may take significant time in a case of the big database!

All stages of replica creation are listed as alerts in HQbird (also sent by email):

<table>
<thead>
<tr>
<th>Order</th>
<th>Date</th>
<th>Severity</th>
<th>Source</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>08/11/2019 15:30 GMT+0300</td>
<td>OK</td>
<td>DIMASTER</td>
<td>Replica (MASTER): reinitialization complete</td>
<td>Prepared replica database file &quot;[database_3].fblib&quot; on 11-Nov-2019, 18:30:00 to send replica to cloud backup. Report file &quot;[database_3].fblib&quot; on 11-Nov-2019, 18:30:00 to 18:30:00 in 10m 34s 638</td>
</tr>
<tr>
<td>2</td>
<td>08/11/2019 15:30 GMT+0300</td>
<td>OK</td>
<td>DIMASTER</td>
<td>Replica (MASTER): calculate file-test finished</td>
<td>Finished calculate file-test for file &quot;[database_3].fblib&quot; on 11-Nov-2019, 18:30:00 in 10m 34s 638</td>
</tr>
<tr>
<td>3</td>
<td>08/11/2019 15:30 GMT+0300</td>
<td>OK</td>
<td>DIMASTER</td>
<td>Replica (MASTER): start calculation file-test</td>
<td>Calculate file-test for file &quot;[database_3].fblib&quot; on 11-Nov-2019, 18:30:00 started at Mon Nov 11 18:30:21 2019 in 0m 34s 638</td>
</tr>
<tr>
<td>4</td>
<td>08/11/2019 15:30 GMT+0300</td>
<td>OK</td>
<td>DIMASTER</td>
<td>Replica (MASTER): initialization in process</td>
<td>Finished file-test &quot;[database_3].fblib&quot; on 11-Nov-2019, 18:30:00 in 10m 34s 638</td>
</tr>
<tr>
<td>5</td>
<td>08/11/2019 15:30 GMT+0300</td>
<td>OK</td>
<td>DIMASTER</td>
<td>Replica (MASTER): initialization in process</td>
<td>Finished calculation file-test for file &quot;[database_3].fblib&quot; on 11-Nov-2019, 18:30:00 started at Mon Nov 11 18:30:21 2019 in 0m 34s 638</td>
</tr>
</tbody>
</table>

**Note**

Please make sure that replica creation process was completed successfully — check Alerts tab!

**Step 3: Setup database for async replication at the replica(slave) server**

After completing the configuration of asynchronous replication on the master server, we need to configure it for the replica database at the replica server instance.

First of all, we assume that you have successfully installed HQbird Enterprise on the replica server. We recommend to use on replica server SuperClassic for Firebird 2.5 and SuperServer for Firebird 3.0 (these are default configurations of HQbird Enterprise).

**Firebird Classic Linux users**: If you run Firebird on replica server in Classic mode on Linux, you need to run additional Firebird replicator process with the command `fb_smp_server -r`.

Second, the replica database should be registered in HQbird FBDATAGuard. If you intend to use automatic re-initialization, you can register some small database (`employee.fdb`) with the required name, and the do re-initialization: as a result, replica database will be automatically transferred from the master server.

Third, we assume that you have managed to setup transfer of logs with Cloud Backup/Cloud Backup Receiver, or with network share.

**Note**

Please note: the database should have replica database GUID before the registration! This GUID is created automatically if you have used link «Reinitialize replica database», but if you are performing manual re-initialization, don’t forget to set it, otherwise will be an error about missing database GUID.
Then complete the replication setup — the only required parameter is a path to the folder with archived replication segments, and by default it is already set — HQbird will create folder with logs near the database:

So, no need to change anything here, just click Save.

Assuming the replica database is configured in D:\DATABASE\DBWREPLICA.FDB, the HQBird will create folder D:\DATABASE\DBWREPLICA.FDB.LogArch, and replica will import replication segment files from it.

Click “Save” and restart Firebird service (to ensure that replication parameters were applied).

After restart, the replica server will start to consume the replication segments from the folder — please note, after the import all processed segments will be deleted. Also, it will create file with the name {DATABASE-GUID} — Firebird stores there some internal information about replication progress.

Note
It is not recommended to store archived replication segments from the different databases into the same folder! Always allocate the separate folder for each pair of master-replica databases!

6.4. Automatic initialization and re-initialization of replica

We recommend using Cloud Backup on the master and Cloud Backup Receiver on the replica to implement the transfer and check integrity of the replication segments through FTP. In this case, it is also possible to implement 1-click re-initialization for the replica database.

If Cloud Backup and Cloud Backup Receiver have the following options enabled (by default), HQbird perform the re-initialization automatically, including restart of replica database:
Parameter “Prefix to name uploaded reini files” should be changed if you intend to initialize several copies of the master database through the single folder – in this case set it should be unique for each database.

In case of the single database, no changes are required.

**How re-initialization works**

If Cloud Backup/Cloud Backup Receiver are configured, it is possible to perform the complete re-initialization with 1 click to “Reinitialize replica database”.

Once clicked, the master HQbird will do the following:

1. Ask you where to store copy of the database (by default it is near the master database, click Ok to store database there).

2. Master database will be copied (with nbackup)

3. The created copy of the database will be set to the replica mode

4. md5 hash-sum will be calculated for the copy

5. According the settings in Cloud Backup (Enable replication should be Enabled), master HQbird will upload database to the specified FTP

Next steps will be done by replica HQbird instance:

1. Once replica HQbird will notice the reini* files in the incoming FTP folder, Cloud Backup Receiver will start the procedure of re-initialization.

2. Processing if usual arch-segments will be stopped

3. The arrived database will be checked — md5 hash-sum will be calculated and compared with the value in the accompanied report file.

4. The existing replica database will be shutdown to disconnect all users

5. New replica database will be copied over the existing database

6. The replica server may require restart to see new replica.

Replica is back to the normal mode.

**Troubleshooting asynchronous replication**

If you have setup asynchronous replication, but it does not work, the first thing is to enable job “Replication Log” on the master and on the replica. This job parses replication.log files, and if there are errors, creates the appropriate alert.
Also, the good thing is to enable “Verbose” option on the replica, and restart Firebird. Verbose will make Firebird to write a lot of details about replication into the replication.log file (near firebird.log).

Usually the text of the error is self-explanatory, but since there are some popular questions which occur regularly, we decide to create the table with the list of main problems with asynchronous replication and ways to resolve it.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible reasons and how to resolve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master part of replication was configured, but folders for operational</td>
<td>HQbird creates these folders automatically, but it requires permissions.</td>
</tr>
<tr>
<td>or archived segments (${dbpath}.LogRepl or ${dbpath}.LogArch) are not</td>
<td>On Windows: these folders should be on local drives, or HQbird and Firebird services must run with</td>
</tr>
<tr>
<td>created</td>
<td>“Run As” with the powerful account (Domain Admin?).</td>
</tr>
<tr>
<td>Master part of replication was configured; folders for ReplLog and</td>
<td>Firebird does not see the replication configuration. Restart Firebird service (all</td>
</tr>
<tr>
<td>LogArch were created, but Firebird does not see the replication</td>
<td></td>
</tr>
<tr>
<td>configuration. Restart Firebird service (all</td>
<td></td>
</tr>
<tr>
<td>Problem</td>
<td>Possible reasons and how to resolve</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>nothing appear there. Replication.log is empty.</td>
<td>connections in case of Classic) to make read the new configuration.</td>
</tr>
<tr>
<td>Master part of replication was configured; there are files databasename.log-000 in ReplLog folder, but no files in LogArch. Also, could be errors about insufficient space or out of space in replication.log</td>
<td>It means that there is no permission for Firebird to access the LogArch folder and create replication segment files (databasename-logarch.000 XXX) there. If LogArch folder on the network share or mounted drive, make sure that Firebird has rights (full access) to access it.</td>
</tr>
<tr>
<td>“Verbose” option on replica is enabled, but replication.log is empty or nor created.</td>
<td>Sometimes Firebird cannot create replication.log or even write to already created file. Try to create it manually and apply necessary permissions to it (especially on Linux). Verbose output should be written to the replication.log every 60 seconds even if there is no segments to import.</td>
</tr>
<tr>
<td>Master part of replication is Ok, but replica does not consume replication segments. Replication.log file is empty.</td>
<td>Replica did not read the new replication configuration. Restart Firebird.</td>
</tr>
<tr>
<td>Master part of replication is Ok, but replica does not consume replication segments. Replication.log contains errors about permissions.</td>
<td>Replica does not have enough permissions to read from the LogArch folder. Set necessary permissions or run replica under powerful account.</td>
</tr>
<tr>
<td>Replica has errors in replication.log “Segment NNN is missing”</td>
<td>Check is there such segment on the replica side, and if it is on the master size. If segment has size = 0 on replica, copy it manually or use “Perform fresh backup” checkmark in Cloud Backup.</td>
</tr>
<tr>
<td>Replica has errors in replication.log about wrong foreign keys and stopped consume segments</td>
<td>It means that replica copy is desynchronized, so some records do not have the appropriate values in referenced tables for the specified Foreign Key. Replica should be reinitialized. If you see this errors often, please contact IBSurgeon support.</td>
</tr>
</tbody>
</table>

### 6.5. Synchronous replication for Firebird

In case of synchronous replication, master server directly inserts committed changes of the master database to one or more replicas databases:
The main features of the synchronous replication are the following:

- Changes are buffered per transaction, transferred in batches, synchronized at commit
- Practical delay is below 1 second
- Follows the master priority of locking
- Replication errors can either interrupt operations or just detach replica
- Replica is available for read-only queries (with caveats)
- Automatic fail-over can be implemented (with HQbird Cluster Manager)

Issues to be considered

- Additional CPU and I/O load on the replica side
- Requires direct and permanent network connection from master to replica(s), 1+Gbps recommended
- Replica can be recreated online, re-initialization of synchronous replication requires stop of master

When to use synchronous replication:

- Custom fail-over cluster solutions with 3+ nodes (especially for web applications)
- Scale performance by moving reads to the separate replica server (report servers, data marts or read-only web representation)
- In combination with asynchronous replication for performance scaling

**Steps to setup synchronous replication**

1. Stop Firebird
2. Create a copy of master database file, switch it to replica mode and copy it to the replica server(s)
3. Setup replica server(s) and database(s) for replication with HQbird FBDataGuard
4. Start replica server(s) — before master server!
5. Setup master server and master database for replication with HQBird FBDataGuard

6. Start master server

As you can see, the downtime required for initialization the synchronous replication is bigger than downtime to configure asynchronous replication, because replica database must be online before master's start.

**Synchronous replication at master and replica**

Synchronous replication is designed to write changes from the master database directly to the replica database. The big advantage of synchronous replication that replication delay can be very small, but the disadvantage is that in the case of the lost connection between master and replica servers there will be gaps in transmitted data.

In this example, the synchronous replica database is on the remote server with IP address `replica server` and path `/data/test2.fdb`.

No setup is necessary for synchronous replication on the replica server, except `gfix -replica {master-guid}` for the replica database to switch it to the replica mode.

**Replication parameters for testing synchronous replication**

In the case of testing synchronous replication of HQbird Enterprise on the production system, we recommend setting parameter `disable_on_error` to true.
It will switch off replication in case of replication error, and the master server will continue to work without replication.

To reinitialize replication the replication log should be analyzed and all initialization steps should be done again.

Also, please enable job “Replication log” in HQbird FBDdataGuard to monitor replication log for errors and warnings:
6.6. How to manually create replica of the database?

Of course, it is always possible to create replica with the simple copy process: stop Firebird on master, copy database file, complete setup of replication on the replica, then start Firebird. However, HQbird supports online replica creation – see details below.

If, for some reason, you cannot use the automatic replica creation (which is available since v. 2018 R2), you can create replica copy of the master database manually.

Starting with HQbird 2018, it is possible to create replica file without stopping the master server, with nbackup. It is easy for asynchronous replication, and it also makes possible to create additional replicas online — i.e., without stopping a master.

Creating copy online (with nbackup)

Let's consider how to create replica for asynchronous replication using nbackup:
1. apply nbackup lock

```
nbackup -l database_path_name -user SYSDBA -pass masterkey
```

2. copy locked database file to create a replica

```
copy database_path_name replica_path_name
```

3. unlock master database

```
nbackup -n database_path_name -user SYSDBA -pass masterkey
```

4. Fixup replica database

```
nbackup -f replica_path_name
```

5. Switch database to replica mode

```
gfix replica_path_name -replica {DATABASEGUID} -user SYSDBA -pass masterkey
```

**What is {DATABASEGUID}?**

Database GUID is the unique identifier of a master database. To find out {DATABASEGUID}, run command `gstat -h`:
To switch database to the replica mode run the following command:

```
gfix disk:\path\mydatabase.fdb -replica {guid} -user SYSDBA -pass masterkey
```

**How to set replica database to the master mode**

To switch database to the normal (master) mode run the same command with the empty {} instead of database GUID:

```
gfix disk:\path\mydatabase.fdb -replica {} -user SYSDBA -pass masterkey
```
Note

If you don't see Database GUID in `gstat -h` output, connect to the master database using Firebird binaries from HQbird distribution (with `isql` or any other application), and run `gstat -h` again.

6.7. How to distinguish master database from replica

Using `gstat -h`

If you run `gstat -h database_name`, the output will contain the keyword “replica” in Attributes section for database configured as replica:

```
Database "D:\O30.FDB"
Gstat execution time Mon Nov 26 17:47:07 2018

Database header page information:
  Flags                   0
  Generation              187842
  System Change Number    15
  Page size               8192
  ODS version             12.0
  Oldest transaction      173630
  Oldest active           185440
  Oldest snapshot         185440
  Next transaction        185441
  Sequence number         0
  Next attachment ID      24975
  Implementation          HW=AMD/Intel/x64 little-endian OS=Windows CC=MSVC
  Shadow count            0
  Page buffers            0
  Next header page        0
  Database dialect        3
  Creation date           Jan 11, 2017 15:12:20
  Attributes              replica

Variable header data:
  Database backup GUID:   {37E7918F-5478-43CF-E3B2-D80B0E7D3F63}
  Sweep interval:         0
  Database GUID:          {BBBD2881-ACDE-4636-CEB2-7EE31AF66CC3}
  Replication master GUID: {BBBD2881-ACDE-4636-CEB2-7EE31AF66CC3}
*END*
Gstat completion time Mon Nov 26 17:47:07 2018
```

For master database there is no special marks in Attributes.

With SQL query to the context variable `SYSTEM.REPLICA`

There is a new context variable in the SYSTEM area, which contains the information about database status:
6.8. Optional parameters for replication

It is possible to specify several additional parameters for fine tuning of the replication process. These parameters can be specified in the "Optional parameters" of replication setup dialog.

1. Size of the local buffer used to accumulate replication events that can be deferred until the transaction commit/rollback. The bigger this value the less network round-trips between master and slave hosts are performed. However, it costs longer replication "checkpoints" (time to synchronize the original database with its replica).

   buffer_size = 1048576

2. If enabled, any error during replication causes the master to stop replicating changes and continue working normally. Otherwise (the default behavior), the master reports an error.

   disable_on_error = false

3. If enabled, replicated records are RLE-compressed before transmission and decompressed on the slave side. It reduces the traffic and (indirectly) a number of round-trips at the cost of extra CPU cycles on both sides.

   compress_records = false

4. If enabled, conflicting records in the target database are modified to match records in the master database. In particular:

   • if there's an insert and the target record exists, it gets updated;
   • if there's an update and the target record does not exist, it gets inserted;
   • if there's a delete and the target record does not exist, it gets ignored.

   master_priority = false

5. Pattern (regular expression) that defines what tables must be included into replication. By default, all tables are replicated.
6. **include_filter**
   Pattern (regular expression) that defines what tables must be excluded from replication. By default, all tables are replicated.

7. **exclude_filter**
   If enabled, tables without primary key (or unique index) excluded from replication. By default, all tables are replicated.

   ```
   exclude_without_pk = false
   ```

8. **alert_command**
   Program (complete command line with arguments) that is executed when the current replication session notices a critical error. This command is executed once per every failed replication session. Please note that the program is executed synchronously and the server is waiting for its completion before continuing its operations.

9. **log_file_prefix**
   Prefix for replication log file names. It will be automatically suffixed with an ordinal sequential number. If not specified, database filename (without path) is used as a prefix.

10. **log_segment_size**
    Maximum allowed size for a single replication segment. It must at least double the specified `buffer_size`.

    ```
    log_segment_size = 16777216
    ```

11. **log_segment_count**
    Maximum allowed number of full replication segments. Once this limit is reached, the replication process is delayed for `log_archive_timeout` seconds (see below) to allow the archiving to catch up. If any of the full segments is not archived and marked for reuse during the timeout, the replication fails with an error.

    Zero means an unlimited number of segments pending archiving.

    ```
    log_segment_count = 8
    ```
Chapter 7

Performance enhancements

7.1. Pool of external connections

HQbird 2018 supports a pool of external connections for Firebird 2.5 and (from 2018R3) in Firebird 3. This pool allows running parallel EXECUTE ON EXTERNAL statements to external Firebird databases.

Note
Please note — this pool is allocated per Firebird instance.

The feature is managed in the firebird.conf:

```
# ===============
# Settings of External Connections Pool
# ===============

# Set the maximum number of inactive (idle) external connections to retain at
# the pool. Valid values are between 0 and 1000.
# If set to zero, pool is disabled,
# i.e. external connection is destroyed immediately after the use.
# Type: integer
#
# ExtConnPoolSize = 0

# Set the time before destroying inactive external connection, seconds.
# Valid values are between 1 and 86400.
# Type: integer
#
# ExtConnPoolLifeTime = 7200
```

From the application point of view, no additional steps are required to use or do not use — it is enabled or disabled in the server configuration, and absolutely seamless for the applications.

The following commands exist to manage pool:

- changes the pool size

  ALTER EXTERNAL CONNECTIONS POOL SET SIZE N

Example — this command sets the size of a pool to 190 connections.
Performance enhancements

**ALTER EXTERNAL CONNECTIONS POOL SET SIZE 190**

- changes the lifetime of the pooled connection

**ALTER EXTERNAL CONNECTIONS POOL SET LIFETIME \(N\) \{SECOND | MINUTE | HOUR\}

Example — this command limits the lifetime of a connection in the pool to 1 hour.

**ALTER EXTERNAL CONNECTIONS POOL SET LIFETIME 1 HOUR**

- clear all pooled connections

**ALTER EXTERNAL CONNECTIONS POOL CLEAR ALL**

- clear the oldest connection in the pool

**ALTER EXTERNAL CONNECTIONS POOL CLEAR OLDEST**

To get information about pool status, new context variables were introduced. The following example demonstrates their usage

```
SELECT
  CAST(RDB$GET_CONTEXT('SYSTEM', 'EXT_CONN_POOL_SIZE') AS INT) AS POOL_SIZE,
  CAST(RDB$GET_CONTEXT('SYSTEM', 'EXT_CONN_POOL_IDLE_COUNT') AS INT) AS POOL_IDLE,
  CAST(RDB$GET_CONTEXT('SYSTEM', 'EXT_CONN_POOL_ACTIVE_COUNT') AS INT) AS POOL_ACTIVE,
  CAST(RDB$GET_CONTEXT('SYSTEM', 'EXT_CONN_POOL_LIFETIME') AS INT) AS POOL_LIFETIME
FROM RDB$DATABASE;
```

7.2. Cached prepared statements

HQbird 2018 has the feature to improve the performance of Firebird (version 3+ only!) engine in case of the many frequent and fast SQL queries: server-side cache of prepared SQL statements.

This feature can be enabled in `firebird.conf` with the parameter `DSQLCacheSize`:

```
# Size of DSQL statements cache.
# Maximum number of statements to cache.
# Use with care as it is per-attachment and could lead to big memory usage.
# Value of zero disables caching.
```
Performance enhancements

# Per-database configurable.
# Type: integer
# DSQLCacheSize = 0

The number specifies how many recent queries for each database connection to cache.

To apply the new value, Firebird restart is required.

By default, cache of prepared statements is 0, it means OFF. We recommend to carefully enable it: start with values like 4, 8, 16, to find the best performance effect.

Note

Please note: enabling cache of prepared statements increases the memory usage.

7.3. TempSpaceLogThreshold: monitoring of big sorting queries and BLOBs

HQbird Enterprise has a new parameter in firebird.conf in Firebird 2.5 and Firebird 3.0:

TempSpaceLogThreshold=1000000000 #bytes

When Firebird sees this parameter, it starts to log to firebird.log queries which produce large sortings: queries with GROUP BY, ORDER BY, etc.

When such query creates the sorting file which exceeds the specified threshold, the following message will appear in firebird.log:

SRV-DB1 Wed Nov 28 21:55:36 2018
Temporary space of type "sort" has exceeded threshold of 1000000000 bytes.
Total size: 10716980736, cached: 1455423488 bytes, on disk: 9263120384 bytes.
Query: select count(*) from (select lpad('',1000,uuid_to_char(gen_uuid())) s
from rdb$types a,rdb$types b, rdb$types c  order by 1)

Total size — the total size of sorting file
Cached — the part of sorting which had fit into temporary space (specified by TempCacheLimit parameter)
On disk — the part of sorting which was stored to the temporary file, which can be cached in the OS memory, or stored on disk (in the folder specified by TempDirectories parameter, or in the default temp folder)
For very big BLOBs the following message will appear in the firebird.log

SRV-DB1 Tue Nov 27 17:35:39 2018
Temporary space of type "blob" has exceeded threshold of 500000000 bytes.
Performance enhancements

Total size: 500377437, cached: 0 bytes, on disk: 501219328 bytes.

Use TempSpaceLogThreshold to find the non-optimized queries with big sortings and big BLOBs. In Firebird 3.0, it also will report large hash sortings.

If you encounter such queries, optimize them either with redesign of SQL query itself, or try to enable parameter SortDataStorageThreshold.

7.4. SortDataStorageThreshold: REFETCH instead SORT for wide record sets

HQbird Enterprise has a new parameter SortDataStorageThreshold in firebird.conf (Firebird 3.0 only):

SortDataStorageThreshold=16384 # bytes

If the size of the record, returned by SQL query, will be more than specified threshold, Firebird will use the different approach for sorting record sets: REFETCH instead of SORT.

For example, we have the following query

```sql
select tdetl.name_detl,
       tmain.name_main,
       tdetl.long_description
from tdetl
join tmain on tdetl.pid=tmain.id
order by tdetl.name_detl
```

with the following execution plan:

```
Select Expression
   -> Sort (record length: 32860, key length: 36)
      -> Nested Loop Join (inner)
         -> Table "TMAIN" Full Scan
            -> Filter
               -> Table "TDETL" Access By ID
                  -> Bitmap
                     -> Index "FK_TABLE1_1" Range Scan (full match)
```

In this case, the size of each record to be sorted is 32860+36 bytes. It can lead to the very big sort files, which will be written to the disk, and the overall query can slow.

With parameter SortDataStorageThreshold=16384, Firebird will use plan REFETCH, where only key is sorted, and data are read from the database:

```
Select Expression
```
Performance enhancements

-> Refetch
  -> Sort (record length: 76, key length: 36)
  -> Nested Loop Join (inner)

This approach can significantly (2-5 times) speed up queries with very wide sorted record sets (usually, heavy reports).

Please note!
It is not recommended to set SortDataStorageThreshold less than 2048 bytes.

7.5. Multi-thread sweep, backup, restore

In HQbird 2020, the possibility of multi-threaded execution of sweep, backup and restore has appeared, which speeds up their work from 2x to 6 times (depending on the specific database). Multi-threaded operations work in HQbird Firebird 2.5 and 3.0 (starting from builds 2.5.9.27143 and 3.0.5.3.31717 respectively), in any architectures — Classic, SuperClassic, SuperServer.

To enable multi-threaded execution, the gfix and gbak command-line utilities have the \texttt{\--par \textit{n}} option, where \textit{n} is the number of threads that will be involved in a particular operation. In practice, choosing the number \textit{n} should be correlated with the number of available processor cores.

For example

\begin{itemize}
  \item gfix \texttt{\--sweep} database \texttt{\--par} 8 ...
  \item gbak \texttt{\--b} database backup \texttt{\--par} 8 ...
  \item gbak \texttt{\--c} backup database \texttt{\--par} 8 ...
\end{itemize}

Also, to control the number of threads and set their default number in \texttt{firebird.conf}, two new parameters are introduced that affect only sweep and restore, but not backup:

```
# Settings for parallel work
# Limit number of parallel workers for the single task. Per-process.
# Valid values are from 1 (no parallelism) to 64. All other values
# silently ignored and default value of 1 is used.
MaxParallelWorkers = 64
```

Example: if you set \texttt{MaxParallelWorkers = 10}, then you can

\begin{itemize}
  \item run gfix \texttt{\--sweep} database \texttt{\--par} 10
  \item run gfix \texttt{\--sweep} database \texttt{\--par} 5 \texttt{\&\&} gbak \texttt{\--c} \texttt{\--par} 5 ...
\end{itemize}

That is, no more than 10 threads will be used in total. In case of exceeding (for example, if you set 6 threads for sweep and 6 threads for restore), for a process that exceeds the limit, the message “No enough free worker attachments” will be displayed.
Thus, to enable the multi-threaded capabilities of sweep and restore, you must set the `MaxParallelWorkers` parameter in `firebird.conf`:

```
MaxParallelWorkers = 64
```

and then restart Firebird.

The `ParallelWorkers` sets the number of threads used by sweep and restore by default if the `–par n` option is not specified.

```
#  Default number of parallel workers for the single task. Per-process.
#  Valid values are from 1 (no parallelism) to MaxParallelWorkers (above).
#  Values less than 1 is silently ignored and default value of 1 is used.
#  ParallelWorkers = 1
```

For example, if `ParallelWorkers = 8`, then starting

```
gfix -sweep
```

without the `–par n` option will use 8 threads to execute sweep in parallel.

### Important

For restore, filling tables from backup is always performed in one thread, and only creating indexes is parallelized. Thus, the acceleration for restore depends on the number of indexes in the database and their size. Also, the `ParallelWorkers` parameter automatically affects the creation of indexes performed by the `CREATE INDEX` and `ALTER INDEX ... ACTIVE` operations.

As mentioned above, these options do not affect backup. The multi-threading of backup is regulated only by the `–par n` parameter in the command line:

- `gbak -b -par 6 ...
- `gbak -b -par 8 -se ...

### Important

If the database is in shutdown single state, when only 1 connection is allowed to the database, then in version 2.5 both sweep and backup with `–par 2` or more will produce an error several seconds after starting:

- sweep — connection lost to database
- backup — ERROR: database ... shutdown (via xnet protocol, a line with this message will not be displayed in the backup log)

This is due to the fact that for these operations an appropriate number of database connections is required, more than 1.

In 3.0, only backup will throw an error “ERROR: database ... shutdown”, sweep will work.

Multi-threaded restore, both 2.5 and 3.0, creates the database in shutdown multi mode, so such errors do not occur. However, there is a risk of connecting other applications from SYSDBA or the owner to the database in the restore process.
Performance enhancements

Notes

- The new parameters in `firebird.conf` only affect sweep and restore, to simplify administration and eliminate ambiguity, it is recommended that you always explicitly specify the `–par n` parameter for gfix and gbak if you need to perform multi-threaded sweep, restore, and backup operations. For example, if you set `ParallelWorkers = 4` and do not specify `–par n`, then sweep and restore will use 4 threads by default, and backup will use 1 thread, because it does not use the values from `firebird.conf` neither locally nor with `–se`.

- The performance improvement does not necessarily depend on the number of processor cores and their compliance with the set value `–par n`. It depends on the number of cores, the Firebird architecture, and the disk subsystem performance (IOPS). Therefore, the optimal value `–par n` for your system must be selected experimentally.
Chapter 8

Encryption support

Since HQbird 2020, HQbird Enterprise includes the encryption plugin and provides support to work with encryption databases in web interface. This feature is supported only in HQBird Enterprise with Firebird 3.0.

**Please note!**
The encryption plugin requires the separate license file, it is sent in the purchase email.

**Please note!**
The encryption plugin can be purchased separately and used with community version of Firebird: https://ib-aid.com/download-demo-firebird-encryption-plugin

8.1. OpenSSL files

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

HQbird Enterprise for Windows already includes necessary binary files from OpenSSL 1.1, in order to use encryption features on Linux it is necessary to install **OpenSSL 1.1**.

**How to encrypt and decrypt Firebird database**

In this short guide below, we will demonstrate the key features of the encryption: how to encrypt your Firebird database on the server, how to implement an encrypted client connection, and perform backup/restore of the encrypted database. The demo of FEPF is fully functional, with the only exception — it is limited until December 30, 2019.

**Demo package with client applications examples**

Please download demo package with client applications examples from https://ib-aid.com/download/crypt/CryptTest.zip

**Stage 1 — Initial encryption of the database**

At the point, we suppose that you have some database to be encrypted. Put unencrypted database to some path, for example, into c:\temp\employe30\employee.fdb

We suppose that all actions are made with 64-bit version of the Firebird 3.0.3+, in case of 32-bit version simply use the files from WinSrv32bit_ServerPart folder.
1. Create the following alias in databases.conf

crypt = C:\Temp\EMPLOYEE30\EMPLOYEE30.FDB
{  
    KeyHolderPlugin = KeyHolder
}

Also, you can declare KeyHolder plugin for all databases at the server, for this add the following parameter to firebird.conf:

KeyHolderPlugin = KeyHolder

or, simply copy firebird.conf at step 2 (see below).

2. Check that the following files to server/plugins from the folder WinSrv64Bit_ServerPart
\plugins

• DbCrypt.dll
• DbCrypt.conf
• KeyHolder.dll
• KeyHolder.conf — this is the text file with keys, it is only for developer’s usage, it should not be sent to end users!

3. Put the following files into Firebird root from the folder WinSrv64Bit_ServerPart

• fbcrypt.dll
• libcrypto-1_1-x64.dll
• libssl-1_1-x64.dll
• gbak.exe
• firebird.msg
• firebird.conf (optional, can be used as an example)

4. Connect to the unencrypted database with isql and encrypt the database:

isql localhost:C:\Temp\EMPLOYEE30\EMPLOYEE30.FDB -user SYSDBA -pass masterkey
SQL>alter database encrypt with dbcrypt key red;
SQL> show database;
Database: localhost:C:\Temp\EMPLOYEE30\EMPLOYEE30.FDB
    Owner: ADMINISTRATOR
PAGE_SIZE 8192
Number of DB pages allocated = 326
Number of DB pages used = 301
Number of DB pages free = 25
Sweep interval = 20000
Forced Writes are OFF
Transaction - oldest = 2881
Transaction - oldest active = 2905
Let's consider the encryption command:

```
alter database encrypt with dbcrypt key red;
```

Here, `dbcrypt` is the name of the encryption plugin, and `red` is the name of the key to being used. Keys are defined in `KeyHolder.conf` file.

Please note — on Linux it is necessary to use quotes and case-sensitive plugin name:

```
alter database encrypt with "DbCrypt" key Red;
```

After that, the database is encrypted with server-side authentication: the keys are located in the file `KeyHolder.conf`.

At the figure below you can see files we have on the server to enable the encryption, and what we need on the client side:

<table>
<thead>
<tr>
<th>On the server's side:</th>
<th>On the client's side (demo - CryptTest.exe) - 32bit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mandatory files:</strong></td>
<td><strong>Mandatory files:</strong></td>
</tr>
<tr>
<td>plugins/dbcrypt.dll</td>
<td>fbclient.dll</td>
</tr>
<tr>
<td>plugins/keyholder.dll</td>
<td>fbcrypt.dll</td>
</tr>
<tr>
<td>DbCrypt.conf</td>
<td>libcrypto-1_1.dll</td>
</tr>
<tr>
<td>libssl-1_1-x64.dll</td>
<td></td>
</tr>
<tr>
<td>libcrypto-1_1-x64.dll</td>
<td></td>
</tr>
<tr>
<td>fbcrypt.dll</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Files for gbak with encryption:</strong></td>
<td></td>
</tr>
<tr>
<td>gbak.exe</td>
<td></td>
</tr>
<tr>
<td>firebird.msg</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Optional files:</strong></td>
<td></td>
</tr>
<tr>
<td>plugins/KeyHolder.conf</td>
<td>(for initial encryption in development mode)</td>
</tr>
<tr>
<td>firebird.conf</td>
<td>(contains parameter to set encryption plugin)</td>
</tr>
</tbody>
</table>
Encryption support

Stage 2 — Connect to the encrypted database with the client application

After the initial encryption, we suppose that the database will be copied to the customer environment, where access to it will be done only through the authorized application.

To imitate such environment, we need to remove (or simply rename) the file with keys (KeyHolder.conf) from the folder plugins.

Without KeyHolder.conf, the encryption plugin will require receiving the key from the connected application. The example of such application is included in the archive with demo plugin — there is a compiled version and full sources for it on Delphi XE8.

The code to initialize encrypted connection is very simple — before the usual connection, several calls should be done to send an appropriate key. After that, the client application works with Firebird as usual.

Run the demo application to test the work with the encrypted database, it is in the folder CryptTest \EnhancedCryptTestClient\Win32\Debug.

Do the following steps:

1. Specify database path or alias in “1. Setup Login”. This database will be used in the next steps.

2. Specify the key name and value to be used. If you have previously used key RED, set Key Name = RED and copy the key value from the KeyHolder.conf file.

3. You can encrypt and decrypt database with the specified key. Please note — encryption takes time, and it requires to have an active connection to the database.

4. Click Execute query to test the connection to the encrypted database with the simple
Please note!
The test application can connect to the encrypted database only through TCP/IP, xnet is not supported.

In the example of the client application, all database operations (connection, transaction start, transaction's commit, query start, etc) are made in the very straightforward way to demonstrate all steps of the operation against the encrypted database. You can use this code as an example for the implementing encryption in your applications.
Step 3: backup and restore of the encrypted database

The full verified backup with gbak.exe is the primary backup method for Firebird databases. The standard Firebird distribution includes command line tool gbak.exe to perform it, however, it will not work with the encrypted database in the production mode (without keys on the server). After the encryption, only authorized applications can access an encrypted database, and standard gbak is not an authorized application.

We all know how important backup and restore for the database health and performance, so, in order to perform backup and restore for the encrypted databases, we have developed gbak.exe with the encryption support, and included it into the FEPF.

It is important to say, that this gbak.exe produces the encrypted backup file: it encrypts the backup with the same key as for the database encryption.

If you run gbak.exe from the plugin files with the switch -?, you will see the new parameters of gbak.exe, which are used to work with the encrypted databases:
Let's consider how to use `gbak.exe` with encrypted databases and backups.

**Backup encrypted Firebird database**

To backup an encrypted Firebird database, `gbak.exe` must provide the key for the server. This key will be used to connect and read the database and to encrypt the backup file.

There are 2 ways to supply the key for `gbak.exe`: store key in the key file or explicitly put it in the command line:

**Example 8.1. Example of backup with the encryption key in the key file**

```plaintext
gbak.exe -b -KEYFILE h:\Firebird\Firebird-3.0.3.32900-0_Win32\examplekeyfile.txt -KEYNAME RED localhost:h:\employee_30.fdb h:\testenc4.fbk -user SYSDBA -pass masterkey
```

Here, in the parameter `-KEYFILE` we specify the location of the files with keys, and in `-KEYNAME` — the name of the key being used. Please note, that the file `examplekeyfile.txt` has the same structure as `KeyHolder.conf`.

If you apply backup with encryption (`gbak -b -keyfile ... -keyname ...`) on the unencrypted database, the backup will be encrypted.

**Example 8.2. Example of backup with the explicit key**

```plaintext
gbak -b -KEY 0xec,0xa1,0x52,0xf6,0x4d,0x27,0xda,0x93,0x53,0xe5,0x48,0x86,0xb9,0x7d,0xe2,0x8f,0x3b,0xfa,0xb7,0x91,0x22,0x5b,0x59,0x15,0x82,0x35,0xf5,0x30,0x1f,0x04,0xdc,0x75, -keyname RED localhost:h:\employee30\employee30.fdb h:\testenc303.fbk -user SYSDBA -pass masterkey
```

Here, we specify the key value in the parameter `-KEY`, and the name of the key in the parameter `-KEYNAME`. It is necessary to specify key name even if we supply the explicit key value.

**Restore the backup to the encrypted Firebird database**

The `gbak` can also restore from the backup files to the encrypted databases. The approach is the same: we need to provide the key name and key value to restore the backup file.

See below examples of the restore commands:

**Example 8.3. Example of restore with the encryption key in the keyfile**

```plaintext
gbak -c -v -keyfile h:\Firebird\Firebird-3.0.3.32900-0_Win32\examplekeyfile.txt -keyname white h:\testenc4.fbk localhost:h:\employeeenc4.fdb -user SYSDBA -pass masterkey
```
Example 8.4. Example of restore with the explicit key

gbak -c -v -key 0xec,0xa1,0x52,0xf6,0x4d,0x27,0xda,0x93,0x53,0xe5,0x48,0x86,
  0xb9,0x7d,0xe2,0x8f,0x3b,0xfa,0xb7,0x91,0x22,0x5b,0x59,0x15,0x82,0x35,0xf5,
  0x30,0x1f,0x04,0xdc,0x75, -keyname RED  h:\testenc4.fbk
  localhost:h:\employeeenc4.fdb  -user SYSDBA -pass masterkey

If you restore from an unencrypted backup file with encryption keys (gbak -c -keyfile ... -
keyname ...), the restored database will be encrypted.
Firebird has a convenient mechanism of cross-database queries: Execute Statement On External (ESOE). For example, the typical ESOE can look like this:

```
EXECUTE STATEMENT 'SELECT * FROM RDB$DATABASE'
ON EXTERNAL 'server:db1' AS USER 'MYUSER' PASSWORD 'mypassword'
```

As you can see, the statement contains username and password in the open form, which is not secure: for example, if ESOE is called from the stored procedure code, connected users can see the password.

The HQbird Enterprise includes an authentication plugin for ESOE allows to establish trusted relationships between Firebird servers and perform the authentication of ESOE without a password:

```
EXECUTE STATEMENT 'SELECT * FROM RDB$DATABASE'
ON EXTERNAL 'server:db1' AS USER 'MYUSER';
```

Let's consider how to install and configure HQbird Authentication plugin for ESOE.

### 9.1. Installation of authentication plugin for ESOE

**Authentication plugin files**

- **Windows**
  - plugins\cluster.dll
  - clusterkeygen.exe
- **Linux**
  - plugins\libcluster.so
  - bin\ClusterKeygen # executable
Authentication plugin for Execute Statement On External

Please note!
The plugin files are already included into HQbird Enterprise, so you don't need to copy them. There are different files for 32 and 64 bit versions of Firebird.

**Configuration**

**In firebird.conf**

First of all, it is necessary to add plugin name (Cluster) to the **AuthServer** and **AuthClient** parameters in `firebird.conf` on all servers which will trust each other:

```
AuthServer = Srp, Legacy_Auth, Cluster
AuthClient = Srp, Srp256, Legacy_Auth, Cluster
```

**Keyfile**

Then, it is necessary to generate keyfile for the plugin. This key should be placed to the all Firebird servers which should trust to each other.

In order to generate keyfile `cluster.conf` run the following command:

```command
C:\HQbird\Firebird30>clusterkeygen.exe > cluster.conf
```

As a result, the key file `cluster.conf` will be generated. It contains 2048 digits key, something like this:

```
```

Then, we need to copy the key file to the all Firebird servers with trusted relationships to the **plugins** folder. Key, created on Windows, can be used on Linux, and vice versa.
Authentication plugin for Execute Statement On External

Please note!
The keyfile name should be exactly `cluster.conf`. It should be located in `plugins` folder of Firebird.

Mapping

In order to use authentication plugin inside the particular database, it is necessary to create mapping between users of cluster plugin and regular Firebird users.

For example, if we run the following ESOE

```sql
EXECUTE STATEMENT 'SELECT * FROM RDB$DATABASE'
ON EXTERNAL 'server:db1' AS USER 'MYUSER';
```

we need to map user `MYUSER` to the actual user in the destination database `db1`. Let's assume we have a user `MYUSER2` in the destination database, in this case we need to create the following command in the destination database `db1`:

```sql
SQL> CREATE MAPPING usr_mapping_cluster1 USING PLUGIN CLUSTER
CON> FROM USER MYUSER TO user MYUSER2;
SQL> commit;
```

As a result, the mapping `usr_mapping_cluster1` will be created in `db1`, to map user `MYUSER` to `MYUSER2`.

Please note!
The both users should exist, even if they have the same name. Otherwise there will be the following error:

```
Execute statement error at attach:
335544472: Your user name and password are not defined. Ask your database administrator to set up a Firebird login.
```

You can create as many mapping as you need. Existing mapping can be found in the table `RDB$AUTH_MAPPING` with the following query:

```sql
SQL> select rdb$map_name, rdb$map_from, rdb$map_to from RDB$AUTH_MAPPING
CON> where RDB$MAP_PLUGIN = 'CLUSTER';
```

<table>
<thead>
<tr>
<th>RDB$MAP_NAME</th>
<th>RDB$MAP_FROM</th>
<th>RDB$MAP_TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>USR_MAPPING_CLUSTER1</td>
<td>MYUSER</td>
<td>MYUSER2</td>
</tr>
</tbody>
</table>
Global mappings

It is possible to create mapping between users for all databases on the server — in this case the following command should be used:

```sql
CREATE GLOBAL MAPPING global_usr_mapping_cluster1 USING PLUGIN CLUSTER
FROM USER MYUSER TO user MYUSER2;
```

In this case, mappings will be stored in security database, to see them use the following query:

```sql
SQL> select SEC$MAP_NAME, SEC$MAP_USING, SEC$MAP_FROM, SEC$MAP_TO
CON> from SEC$GLOBAL_AUTH_MAPPING where SEC$MAP_PLUGIN = 'CLUSTER';
```

<table>
<thead>
<tr>
<th>SEC$MAP_NAME</th>
<th>SEC$MAP_USING</th>
<th>SEC$MAP_FROM</th>
<th>SEC$MAP_TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL_USR_MAPPING_CLUSTER1</td>
<td>P</td>
<td>MYUSER</td>
<td>MYUSER2</td>
</tr>
</tbody>
</table>

Role mappings

In order to map user to the role in the destination database, it is necessary to create 2 mappings:

```sql
CREATE MAPPING USR_CLUSTER9 USING PLUGIN CLUSTER
FROM USER MUSER TO ROLE RDB$ADMIN;
```

```sql
CREATE MAPPING USR_CLUSTER_X USING PLUGIN CLUSTER
FROM ANY USER TO USER MYUSER;
```

How to test

The following query can be used to test the work of the authentication plugin for ESOE:

```sql
execute block
returns (CUSER varchar(255), CCONNECT bigint, CROLE varchar(31))
as begin
execute statement
'select CURRENT_USER, CURRENT_CONNECTION, CURRENT_ROLE from RDB$DATABASE'
on external 'server:db1'
into :CUSER, :CCONNECT, :CROLE;
suspend;
end
```

As a result, this query will return username, connection id and user role from the destination database db1.
Chapter 10

RSA-UDR — security functions to sign documents and verify signatures

HQbird Enterprise includes RSA-UDR which contains the set of useful security functions. These functions can be useful to protect documents (stored as varchars, BLOBS and even external files) with digital signature.

Please note!
To use RSA-UDR functions, you need to register them in your database with an appropriate SQL script. The script is available in `plugin\UDR\crypto.sql`

Let's consider functions from this library and examples their usage.

<table>
<thead>
<tr>
<th>Function Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIN2HEX</td>
<td>Convert binary representation to HEX</td>
</tr>
<tr>
<td>BIN2HEXB</td>
<td>Convert BLOB binary representation to HEX</td>
</tr>
<tr>
<td>CRC32</td>
<td>Calculate checksum</td>
</tr>
<tr>
<td>CRC32B</td>
<td>Calculate BLOB checksum</td>
</tr>
<tr>
<td>DECODE_BASE64</td>
<td>Decode to Base64</td>
</tr>
<tr>
<td>DECODE_BASE64B</td>
<td>Decode BLOB to Base64</td>
</tr>
<tr>
<td>ENCODE_BASE64</td>
<td>Encode to Base64</td>
</tr>
<tr>
<td>ENCODE_BASE64B</td>
<td>Encode BLOB to Base64</td>
</tr>
<tr>
<td>HEX2BIN</td>
<td>Convert HEX to binary</td>
</tr>
<tr>
<td>HEX2BINB</td>
<td>Convert NEX BLOB to binary</td>
</tr>
<tr>
<td>MD5</td>
<td>Calculate MD5 hash sum</td>
</tr>
<tr>
<td>MD5B</td>
<td>Calculate BLOB MD5 hash sum</td>
</tr>
<tr>
<td>RSA_PUBLIC_KEY</td>
<td>Generate public key</td>
</tr>
<tr>
<td>RSA_PRIVATE_KEY</td>
<td>Generate private key</td>
</tr>
<tr>
<td>RSA_SIGN</td>
<td>Sign object</td>
</tr>
<tr>
<td>RSA_VERIFY</td>
<td>Verify the signature</td>
</tr>
</tbody>
</table>
### Function Name | Description
--- | ---
SHA1 | Calculate SHA
SHA1B | Calculate SHA for BLOB
SHA256 | Calculate SHA256
SHA256B | Calculate SHA256 for BLOB

Let's consider the simplified example how to use these functions to sign some document and verify the signature.

For simplicity, we will put the document, private key, public key, digest (hash sum of the document) and signature will be in the same table, in the single column:

```sql
SQL> show table TBL;
DOC BLOB segment 80, subtype BINARY Nullable
DIGEST VARCHAR(32) CHARACTER SET OCTETS Nullable
SALTLEN INTEGER Nullable
PRIVATE_KEY VARCHAR(2048) CHARACTER SET OCTETS Nullable
SIGN VARCHAR(1024) CHARACTER SET OCTETS Nullable
PUBLIC_KEY VARCHAR(512) CHARACTER SET OCTETS Nullable
BAD_SIGN VARCHAR(1024) CHARACTER SET OCTETS Nullable
```

Then, let's go through the example:

```sql
-- First, we will connect to the database:
C:\HQbird\Firebird30>isql localhost:c:\temp\rsatest.fdb -user SYSDBA -pass masterkey
Database: localhost:c:\temp\rsatest.fdb, User: SYSDBA

-- and then we will check that functions are registered
SQL> show functions;
Global functions
Function Name Invalid Dependency, Type
================================= ======= =====================================
RSA_PRIVATE_KEY
RSA_PUBLIC_KEY
RSA_SIGN
RSA_VERIFY
SHA256

-- clean the test table
SQL>delete from tbl
SQL>commit;

-- generate private key and write
-- it into table TBL (normally, the private will be kept in the - secret place)
SQL>insert into tbl(PRIVATE_KEY) values(rsa_private_key(1024));
```

207
-- generate public key
SQL> update tbl set PUBLIC_KEY = rsa_public_key(PRIVATE_KEY);

-- create BLOB document
SQL> update TBL set DOC='testtesttest';

-- and calculate its digest
SQL> update tbl set digest = sha256(doc);

-- sign document and remember its signature
SQL> update tbl set sign = rsa_sign(digest, PRIVATE_KEY, 8);

-- check the signature
SQL> select RSA_VERIFY(SIGN, DIGEST, PUBLIC_KEY, SALTLEN) from tbl;

RSA_VERIFY
==========
<true>

-- as you can see, signature is valid

-- change the document (BLOB)
SQL> update TBL set DOC='testtesttest222';

-- recalculate its digest
SQL> update tbl set digest = sha256(doc);

-- check signature
SQL> select rsa_verify(sign, digest, PUBLIC_KEY, 0) from tbl;

RSA_VERIFY
==========
<false>

-- we can see that protected document was changed

Examples of BIN2HEX and HEX2BIN functions

SQL> set list;
SQL> select bin2hex('Test string') from rdb$database;

BIN2HEX 5465737420737472696E67

SQL> select cast (hex2bin('5465737420737472696E67') as varchar(32))
CON> from rdb$database;

CAST  Test string
10.1. How to use RSA-UDR security and conversion functions

In general, RSA-UDR functions allow to seal electronic documents of all types (DOC, PDF, XML, JPG, PNG, etc), and then detect unauthorized changes.

Conversion functions make easy BIN→HEX and HEX→BIN conversions, as well as Base64 encoding and decoding.
Appendix A: Support contacts

We will answer all your questions regarding HQbird FBDataGuard. Please send all your inquiries to support@ib-aid.com

Please note, that customers with active Firebird Support have the priority in the technical support https://ib-aid.com/en/firebird-support-service/