Firebird and IBExpert White Paper

3rd party backup solutions on IFS servers and why we explicitly advise against it!

Holger Klemt, January 2022

Our servers do exactly what they are supposed to do and, because nothing else is running on them, they are extremely stable. It is not uncritical to backup a Firebird database during operation by such external 3rd party software. Technically, the 3rd party software requires the Firebird service to be terminated, albeit briefly. Unfortunately, the process cannot be forced to end in all versions with all configurations without negative effects. However, many 3rd party software systems think they know better and terminate the service through the operating system, even if the Firebird service is under heavy load and still has to write database content. In a Firebird database however, the combined contents of the database file and RAM are always relevant for a restore at operating system level.

Here is an example from our own experience:

A serious database error occurred at a customer's, where the online store works with a Firebird database as the backend, and is also used by 80 stores and many of the total 1700 employees.

The previous solution was based on a Linux cluster, which supposedly ensured 100% reliability. About 4 years ago, a worst case scenario occurred at this very company and resulted in the server, as well as the other cluster node, leaving completely corrupted databases on both disks. Also the database in the RAID was equally corrupted because the cluster distributed the reference file, whether defect or not. Technically it was impossible to determine why this happened, but it caused the central system to be offline for 3 days until, with our help, the database could be restored from an old previous version and was able to work again.

The company then immediately switched to our IFS servers and has encountered no further problems for the past 4 years. Due to the paramountcy of the servers, both existing IFS servers will now also be replaced 4 years later by IFS servers of the latest generation, as recommended by ourselves.

We have created hourly backups on the IFS server, which ensures that all data is available every hour on an identical database server without any critical end-of-service commands. The databases are not that large, so the hourly backups are complete full backups, transferred via FTP from the master to the slave and restored there, thus constantly being tested for consistency.

Working closely with this company's development department, we have also realized transactional real-time replication from master to slave. This has also been running for 4 years without interruption, so that both servers in their data center would have to be simultaneously irrevocably destroyed in different fire zones in order to cause any loss of data.

All IFS servers are configured in such a way so that in the event of a failure of the master server, the IP address of the slave is switched to the master using simple scripts, should the master still not be able to run after rebooting.

A 3rd party backup solution lulls customers into a false sense of security - it all sounds good, but it's not! 3rd party backup solutions don't understand the transaction technology in Firebird that allows backups in real time without ending the process, but instead try to freeze the system with some drivers and master processes, in order to then backup files that they think need to be backed up. The negative realization that there is no valid database file at the end is usually recognized when it is least expected and certainly not needed.

In addition to the backups from the master to the slave, following a successful backup our scripts also transfer an extra backup copy onto an FTP/SFTP server in the customer's local network, so that this file, with or without our help, can also be quickly restored as a database server, should both IFS servers be destroyed by a worst case scenario.

We therefore do not support the use of a 3rd party backup solution on IFS servers. Should this nevertheless be installed, under the Remote DBA package we would limit any worst-case scenario support to restoring the operating system to its as-delivered state. Then, if the database supplied by the backup solution does not work, we will have to charge separately for our assistance at our general hotline rates.

So you might find it necessary to solve a problem which would never occurred in the first place, had you not installed a 3rd party software.

PS:

I know that many companies' management like to refer to such universal promises of the major vendors as a reference, but let's take such trivial things as the log4j, or currently since January 1, 2022 the MS Exchange Server bug.

The cause of the Exchange Server error occurred worldwide, although you can explain to a first-year developer the reason why what Microsoft did there should never be done that way. But why it was done by Microsoft at all is unclear.

To summarize: the 2-digit year, i.e. currently 22, is multiplied by 100 million and then followed by further values for month, day, time, etc.

In 2021, the year digits were 21, so the value was about 2.1 billion. This still fits into the maximum value for a 32 integer, which is 2147483647. However, the value may not be increased. Since January 1, 2022 however, this results in a value of approx. 2.2 billion.

It is incredibly embarrassing that Microsoft only noticed this after it had already brought tens of thousands of customers worldwide simultaneously to a communication standstill of their e-mail.