



Richard Carlton Consulting

1941 Rollingwood Drive • Fairfield, CA 94534
(707) 422-4053 • www.RCConsulting.com

Fairfield
Sacramento
Santa Clara
Palmdale

Recommended Backup Strategy for FileMaker Server 10 and 11 for Macintosh & Windows

Updated September 2010

This document provides a single cohesive resource for managing and understanding the backup strategy of a FileMaker database server. It deals with misconceptions, planning, hardware requirements, and the correct procedures for restoring databases after a crash.

What should I do to backup a FileMaker Pro database?

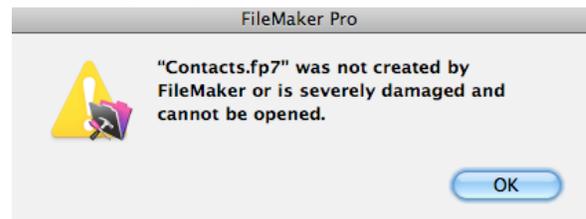
Misconception: *“Any third party (storage-level) backup software will do.”*

The goal of any backup strategy is to provide the complete backup data for those instances of failure or loss of your files. However, conventional backup strategies (including Time Machine and Shadow Copies) cannot meet the needs of FileMaker Server. Current IT doctrine dictates the use of incremental storage-level backups utilizing a corporate network and dedicated backup servers, but this methodology alone is completely useless for hosted database files. Many end-users of FileMaker Server fail to understand that, since a hosted FileMaker database is always open, creating a copy of that file results in a backup that is corrupt and unstable. **In the case of FileMaker databases, an administrator must always use the built-in backup scheduling feature of FileMaker Server to make clean and complete backups.**

What should I do when a Database Crashes?

Misconception: *“If a server or database crashes, simply restart the server or database and you’re back in business.”*

FileMaker, Inc. specifically cautions against simply restarting a crashed database and putting it back into service. Even if it is usable, a crashed database most likely will be corrupted. That database may even successfully open in FileMaker Server with no outward indications that corruption has occurred. Continuing to use the database after a crash means that – sooner or later – file corruption will cause your database to become unstable and you will lose data. FileMaker Inc.’s policy on a crash is to **ALWAYS restore from the last good backup**. RCC strictly follows this policy as well. Take the database that was running and don’t use it. Delete it completely or archive it only to retrieve the newest data, but never use it in production again.



I use FileMaker Pro all the time without the need to buy FileMaker Server.

Misconception: “*FileMaker Server is not needed for small offices with only a couple of database users. FileMaker Pro can share (a.k.a. host) my database(s) with several other FileMaker users.*”

Is your data is worth more to you than a \$1000? If so, then you need FileMaker Server. Twenty years ago, there was no such thing as FileMaker Server, and the only way to share a database was to use “peer to peer” sharing in FileMaker Pro. But this method has some serious limitations and some real liabilities as well. Unfortunately, some people still insist on using this 20-year-old capability for mission critical databases. **The bottom line is that FileMaker Pro cannot provide automatic backups to a database.** This means that people who use this method for hosting a database do not have current backups of their database. When confronted with a crash, and the potential massive data loss because they don't have a backup, these people almost always just decide to use the crashed database. This is fundamentally flawed logic.

HARDWARE

Choosing the right backup media is important. While tape backups have been an IT standard for years, tape does not afford you the flexibility needed to recover quickly in the event of a crash. DVD-Rs, CD-RWs and other removable storage media are also impractical. These are relatively slow and require you to manually swap out and archive the storage media. Instead, we will use **two additional hard drives that are NOT configured together as a RAID system.** If you must use RAID, you must consider any RAID system as a single hard drive. Why? Because while RAID is designed to protect solely against hardware failure, it DOES NOT protect a database from file corruption or from accidentally overwriting or deleting data, nor does it provide a restore point for the OS. A RAID system would simply write the bad data to both drives, leaving no historical backup.

While internal hard drives work well for backups, a good alternative is to consider full-size external storage devices such as “ESATA,” “1394-Firewire,” or “USB 2.0” hard drives. These devices contain a 3.5” hard drive similar to the internal drives, except that these units are external – so they are easily moved between computers in the event of an emergency. The downside of external enclosures is that some enclosures are cheaply made with low quality power supplies (power brick). For example, RCC has seen a huge number of Chinese-made external power bricks fail on external enclosure boxes. For this reason, always try to buy a reputable enclosure from a trusted supplier. The cheapest enclosure is frequently not the best unit for reliability.

FILEMAKER BACKUP STRATEGY



Three types of backups: “Bootable Backups”, “Local Database Backups”, and “Offsite Database Backups.”

RCC STRONGLY RECOMMENDS USING ALL THREE BACKUP TECHNIQUES ON ANY MISSION CRITICAL FILEMAKER SERVER.

You will need two backup drives. The Bootable Backup drive should have at least the same storage capacity as the Boot Drive. The Database Backup drive will retain 200 copies of the database(s), so the drive capacity should be at least 200 times the potential size of the databases (plus 25% as a safety factor).

Example of determining size requirement: We discover that all our databases together total 500MB. Expecting moderate growth, we figure double the actual size as the potential size of each backup (1GB). $1\text{GB} \times 200 = 200\text{GB}$. We then add 25% (50GB) as a safety factor, leaving us with 250 GB as our minimum hard drive storage capacity.

For mission critical database servers, RCC recommends a three-drive configuration. *For those who want to use RAID, this means you will need three separate RAID volumes.*

Drive/Volume #1 – Boot Drive: This drive acts as the primary system drive and contains the Operating System, along with the FileMaker Server installation itself and the master databases.

Drive/Volume #2 – Database Backup Drive: This drive acts as a repository for the backups created by the FileMaker Server backup schedules. Typically, this drive will contain both hourly and daily backups of the database(s). This drive is NOT bootable, and typically does not contain any information other than the backup copies of the databases.

Drive/Volume #3 – Bootable Backup Drive: This drive is a complete, bootable copy of the Boot Drive. Typically, the process to create this backup will be run manually. This drive will be used if the Boot Drive fails, but it will not contain any useful copies of the database – those will be drawn from the Database Backup Drive. The Bootable Backup drive can also be used to recover from irreversible system updates or other changes that have caused problems with FileMaker Server.

BOOTABLE BACKUP

Restoring service to a damaged FileMaker Server installation can be tricky, especially if you are running a full deployment of FileMaker Server. The Web Publishing Engine, SSL certificates, and PHP modules add complexity to installation and configuration. The most common failures of FileMaker Server are typically caused by Operating System updates, either from Apple or Microsoft. The next common failure is a crash of the hard drive itself. In our experience, having a third hard drive that contains an identical copy of the first hard drive (except that the databases themselves will be out of date) will mitigate both of these issues. This backup is normally left alone, and is only refreshed after any significant software update is made to the system drive.

RCC uses SuperDuper! for Bootable Backups on the Macintosh.
(<http://www.shirt-pocket.com>)

RCC uses Copy Commander for Bootable Backups on the Windows.
(<http://www.v-com.com>)

RESTORING THE BOOTABLE BACKUP

If the Boot Drive fails or FileMaker Server goes awry, you can reboot the server from the Bootable Backup drive. Depending on your situation, you will either physically replace the Boot Drive with the Bootable Backup drive, or simply boot directly from the Bootable Backup. Once the new drive is up and running, stop FileMaker Server and restore from the last good backup. Then restart FileMaker Server, and you're set. You will then be able to restore the original hardware configuration as planned maintenance.

LOCAL DATABASE BACKUPS

RCC frequently sees customers that do not use the backups in FileMaker Server, or only the default schedule of one backup per day. In reality, exclusively deploying Daily backups is unacceptable in critical database applications. Alternately, deploying only Hourly backups is typically insufficient for recovering from an unnoticed database incident (i.e. an incident that may have happened a couple of days ago). A complete backup plan includes both Hourly and Daily backup schedules.

Enabled	Name	Type	Last Completed	Status	Next
<input type="checkbox"/>	Backup Drive - Daily	Backup	8/5/10 11:05 PM	OK	Disab
<input type="checkbox"/>	Backup Drive - HalfHour	Backup	8/6/10 10:35 AM	OK	Disab

Details for: Backup Drive - Daily

Schedule type	Backup
Schedule name	Backup Drive - Daily
Databases to back up	All databases
Backup folder	filemac:/Database Backups/FileMaker Backups/Daily/
Maximum backups to keep	99
Verify backup integrity	Disabled
Clone the backup	Disabled
Frequency	Daily
Start date	7/28/10
End date	None
Repeat	Run every day, Once per day starting at 11:05 PM
Email notifications	Disabled
Email addresses	N/A

Details for: Backup Drive - HalfHour

Schedule type	Backup
Schedule name	Backup Drive - HalfHour
Databases to back up	All databases
Backup folder	filemac:/Database Backups/FileMaker Backups/HalfHour/
Maximum backups to keep	1
Verify backup integrity	Enabled
Clone the backup	Disabled
Frequency	Daily
Start date	7/28/10
End date	None
Repeat	Run every day, Every 1 Hours 12:35 AM - 11:35 PM
Email notifications	Disabled
Email addresses	N/A

- FileMaker Server Backup Schedules

Richard Carlton Consulting recommends scheduling an Hourly backup from 12AM to 11PM and a separate Daily backup at 11PM – both kept on the Database Backups drive. Mission critical systems should also include a scheduled backup at the bottom of every hour to the Boot Drive, designated as the Half Hour backup. FileMaker Server 10 and 11 allow the administrator to choose the backup retention level for each schedule (up to 99 copies). RCC recommends using the maximum retention possible (99x) for Hourly and Daily Backups; the Half Hour backup is typically set to retain only one copy. At least one of the schedules should include a database

consistency check – typically the Hourly or Half Hour Backup. For the particularly paranoid, we recommend maintaining a smaller set of Hourly and Daily backups on the Boot Drive as well.

To summarize the recommended strategy: The administrator will create a schedule for Hourly backups from 12AM to 11PM, set for the maximum retention level possible. The administrator will also create a schedule for Daily backups, set for 11PM every day, with a similar retention level. The Half Hour backup will be configured with a retention level of one, and executed hourly from 12:30AM to 11:30PM. Either the Hourly or the Half Hour schedule will include a database consistence check.

If adherence with corporate IT policy requires enterprise-level backups, configure that service to include only the Daily backups. If the policy requires a backup of the entire Database Backups drive (which includes the Hourly backups), then IT will likely receive several Gigabytes of data each day. Fortunate for systems that use compressed backups, FileMaker databases generally compress by about 75%.

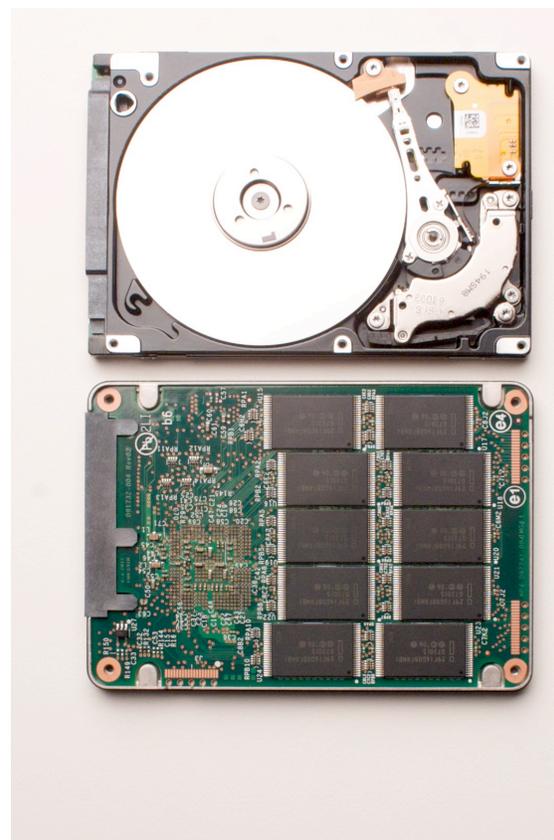
IF DATABASE BACKUPS TAKE TOO LONG

Sometimes FileMaker users will not schedule FileMaker Server to create frequent backups because their databases are large and take too long to backup. The database runs slowly when backups are occurring. The reason a database takes too long to backup is that insufficient investment has been made into the FileMaker Server hardware. A server with slow drives, or without RAID will have a difficult time backing up a multi-gigabyte database quickly. Users have a number of valuable new and affordable technologies to assist in backups. Below are some good ideas.

- Build out and configure a RAID 5 external enclosure with ESATA connection to the Server. Make sure to use speedy drives (at least 7200 RPM).
- Use Solid State Drives (SSD), either singly or in a RAID Configuration.

Case Study: RCC recently had a customer that had a 1.7GB database, using a slow Mac Mini with Firewire 400 for their backups, which ran every 30 minutes. This system contained mission critical financial data, so frequent backups were essential. We replaced that setup with a standard Mac Pro iCore7, at 2.8GHz, with internal non-RAID SSD drives. This resulted in the backups taking 12 seconds to complete, versus 6 minutes. This customer used two SSDs and one 7200 RPM hard drive. One SSD was assigned to run the OS, FileMaker Server software and the live databases. The 2nd SSD was the database backup drive, and the 3rd drive (the slower 7200 drive) was the bootable backup. Backups would read from one SSD and write to the other SSD. This new server cost the customer \$5000. They made this money back in 3 weeks through the time savings produced.

Photo: Top: a conventional spinning disk hard drive. Below: the Solid State hard drive running 20X faster.



RESTORING DATABASE BACKUPS

Using the Admin console, find the database you need to replace and close it. Then use the “Remove” action to remove it from the active folder (this timestamps the file and archives it to a folder named “Removed by FMS”). Next, in the “Related Tasks” column on the left, select “Upload a Database.” This will take you through the process to select and restore a backup file. Refer to the Database Backups section for the location of the backups.

OFFSITE DATABASE BACKUPS

Maintaining offsite database backups is important, and is now easier and more cost effective due to improvements in the speed of internet connections. We have had customers call our offices in a panic to report that someone stole their computers, including the FileMaker Server and its backup hard drives. Theft is a real threat, as is fire. Offsite backups make this danger manageable. RCC uses several different servers for offsite backups. One of the easiest is called dropbox.com. This is an online service designed to synchronize a folder on a computer or server. This provides offsite backup capabilities and has proven to be very reliable. Think about writing one copy of your database per day to an offsite backup. If the database is overly large, you may want to consider “zipping” the database before sending it across the internet. Scripting an automatic zip function can take a bit of work, so contact your local FileMaker consultant or IT support staff for assistance in creating a automatic batch script that will zip your database and move it to Dropbox once a day.

COMPLETE SUMMARY

- (1) Purchase the server and three hard drives.
- (2) Set up the hourly, daily, and half-hour backups to the Database Backup drive as described above.
- (3) Install bootable backup software and periodically make a “mirrored” and “bootable” backup of the Boot Drive onto the Bootable Backup drive.
- (4) Check regularly that the scheduled backups are operating normally.
- (5) Review the process for restoring backups; you will need it sooner or later.

F.A.Q. – FileMaker Server and Backup Questions

- (1) **I use a swappable hard disk (i.e. Iomega Rev drive) and my backups aren't reliable.**
The path name of the directories on the backup drive must be consistent among the cartridges. Additionally, the permissions must be set correctly.
- (2) **My backups won't work on my Mac.** Either the pathname is wrong, or the permissions are. FileMaker Server does not recognize an external drive unless you un-check the "Ignore ownership" box on the Get Info screen. After permissions are enabled on the drive, first set the group to "fmsadmin" and then set the owner to "fmserver." If you still have trouble, use the following Terminal command to set permissions (replace the path with your own backups location path):

```
sudo chown -R fmserver:fmsadmin "/Volumes/Database Backups/"
```
- (3) **Can I just backup across the network to another server?** Actually, you can backup across the network. However, getting the permissions right on the destination volume can be tricky. An alternative is to run a local backup and then, AFTER FileMaker Server completes the backup, use an automated FTP program to push that backup to the remote server. There are a number of techniques that combine FileMaker Schedules, ZIP, and FTP (or some other form of remote file backups) for offsite backups.
- (4) **I asked my IT department to help me purchase a new Server, and they say that I need a machine with RAID. Do I really need this?** RAID can be used successfully, but RAID can really cause big problems if it is your server's only form of backup. The most common type of RAID is to have one drive "mirrored" or copied to the other in real time (RAID 1 or RAID 5). If one hard drive fails, then the other drive is there for you. This in itself does not retain historic data and hence will not protect you from file corruption or accidental data loss caused by user error.

If you ask for two internal hard drives, and your IT department gives you two drives set up for RAID, then you need to have the RAID configuration removed or have an extra non-RAID drive installed. The non-RAID drive can be used as the Database Backups drive.

- (5) **I need three drives for my FileMaker Server, but my server has just one. How do I add the drives? What about External Drives?**

There are two ways of adding drives: internally or externally. Your server may already be set up to accept additional drives internally. SATA drives are now the standard for internal storage; if you have extra drive bays but no free SATA ports you can easily install a SATA card for your SATA hard drive, in a PCI or PCIe slot. External drives will most likely be "USB 2.0," "ESATA," or "1394-Firewire." ESATA is by far the fastest (the same speed as internal SATA), followed by FireWire 800, 400, and then USB 2.0.

Definitions:

FileMaker Pro (a.k.a. FileMaker Client): Database software used by users to access a FileMaker database. A database file may be hosted “peer to peer” by FileMaker Pro, but this provides NO automatic backups and is not recommended.

FileMaker Server: Software designed to host FileMaker Pro databases to many users, and to provide robust automatic backups. Sometimes the term “FileMaker Server” will be used to refer to the piece of hardware that is running the FileMaker Server software.

Backup (for the purposes of this document): A copy, created at a specific date and time, of a database or set of databases.

RAID: A technology that combines a set of hard drives to increase speed and/or reliability.

Bootable Backup: A hard drive which is configured with the operating system, and configuration to allow it to be used to run a server, in case the normal or primary boot drive (e.g. ‘C’ Drive) has failed or is unusable.

Local Database Backup: Database copies residing on the FileMaker Server, on a locally mounted hard drive or volume.

Offsite Database Backup: Database copies residing in a remote location, providing backup in case the FileMaker server and its local database backups are lost or destroyed (by fire, theft, etc.)

SATA: Standard connector/interface used by currently modern hard drives. This standard replaced IDE and ATA drives (which are sometimes referred to as “PATA” drives).

ESATA: External version of the SATA connector/interface used by currently modern hard drives. ESATA connectors attach to external hard drive cases, which typically contain a SATA drive.

USB: A type of external connection interface. The current standard is USB 2.

Firewire: A type of external connection interface. Also known as “1394”, Firewire comes in several flavors, such as Firewire 400, Firewire 800, with later versions much faster. Firewire is less demanding of the computer, and runs at much higher speeds than USB. For greater reliability, use Firewire.