文件服务器--日志监控

目录

[1. 访问日志 1](#_Toc430953590)

[2. 执行日志 2](#_Toc430953591)

日志监控分为访问日志和执行日志，访问日志记录用户每次请求文件操作的详细信息，而执行记录后台的异常信息。

# 访问日志

访问日志可以选择是否启用，勾选启用并保存及开启访问日志功能。启动访问日志后文件服务器会记录链接文件服务器的请求信息。请求信息主要包括：客户端IP、登录的用户名、操作类型、请求的URL、对应操作的文件内容、操作开始时间和操作结束时间。



访问日志可以用于查看每次用户访问文件服务器的具体操作信息，在上图中日志信息主要是本地上传附件到“test”模块下。访问日志记录数过多可以点击“清空”按钮进行清空数据操作，还可以根据指定的条件刷选日志信息。



可用的过滤条件：

client=127.0.0.1

requestUser= #UAP#

operType= POST

requestURL=/fs/service/test/files

content= test#c7a39695-0f12-4979-a9c8-cf1e9f93e491

startTime=2015-09-25 14:03:02

endTime=2015-09-25 14:03:03

# 执行日志

当UFS功能出现异常时，可以通过执行日志来查看具体的日志信息，进而排查错误。执行日志的功能是将后台日志文件的最新内容显示在页面上，方便远程查看错误信息。执行日志中默认最多加载最新的500行日志内容。在加载的日志中可以通过搜索“@UFS”字符串来快速定位文件服务器的错误信息。执行日志默认加载的是文件服务器专有的日志文件/nclogs/server/uapfs.log， 若该文件不存在则加载/nclogs/server/nc-log.log。执行日志可以按行数过滤， 所输入的行数为日志文件的最后的N行， 输入的函数需要小于500， 大于500时候只会显示最新的500行的内容。

