按项目建立可撤销的只读交付范围与访问验收

完整操作教程 · 参考固定 · 往返恢复验收

外部合作者需要查看结果时，先把“能看什么、从哪里看、到期如何撤销”写成一份清单。本文用项目副本和只读验收说明边界，避免为了省事开放整个课题目录。

运行边界：ACL示例仅用于经批准的临时目录；已读到的数据副本无法通过撤销访问收回。

先定义交付对象，不要从 chmod 开始

“只读访问”不是把目录权限改成 755 就算完成。Linux 的目录读取权限允许列出名称，执行权限允许沿路径进入，文件读取权限允许查看内容；目录写权限又可能让合作者创建、删除或改名文件。一个用户对上级目录没有执行权限，即使目标文件本身可读，也可能无法到达；反过来，对父目录开放过宽，会暴露其他项目名称。Docker只读挂载能限制容器通过该挂载写入，但不能替代宿主机路径权限，也不保护通过其他挂载或服务暴露的数据。先画出从账号到项目目录的路径，再决定是提供只读副本、受控下载，还是在独立共享目录中查看。

建议把交付拆成三层：原始数据、分析中间文件、批准公开给合作者的结果。通常外部合作者只需要第三层中的图表、去标识汇总表和说明文档。若下游必须复核中间结果，应逐项列出文件名和用途，不要默认开放整个工作目录。对于含个人信息、未发表数据、受合作协议限制的样本，先确认数据管理责任人和协议允许范围。技术上能访问不等于法律、伦理或项目管理上允许共享。

建立按项目、按期限的访问清单

每次交付都应有一张最小权限表：项目编号、接收人账号、允许访问的目录、可读文件类型、是否允许复制下载、开放起止时间、责任人和撤销方式。不要把账号密码通过文章、邮件附件或共享表格传递。优先使用个人账号和项目组，不要多人共用一个账号；这样才能知道谁访问了什么，也便于人员离组时撤销单个成员。临时协作者不应继承课题组所有项目的共享组。

常见做法是把经批准的结果复制到一个新的交付目录，原始目录仍由课题组自己控制。副本可以带有交付日期和版本号，例如 delivery_2026-11-15_v1，并生成文件清单、摘要哈希、README和许可说明。若采用软链接，需要确认目标路径不会沿链接回到原始数据，也不会因目录移动造成权限旁路。若使用ACL，应同时查看文件和每一级目录的访问控制项；ACL mask会影响组与命名用户权限的有效上限，不能只凭命令执行成功就判断权限正确。

对象	建议策略	验收证据
原始FASTQ/H5AD	默认不对外开放	外部账号无法列出或读取
经批准结果副本	个人账号只读、期限明确	能读目标文件但不能创建或删除
项目说明与清单	与结果一同交付	版本、摘要、用途可追踪
访问日志	仅管理员可读	可识别账号与时间，不含数据正文

在普通账号下做正反两类测试

权限管理员看到的结果不代表外部合作者看到的结果。测试应使用一个没有管理员权限的临时账号，分别验证允许和禁止的操作。正向检查：可以进入交付目录、列出批准的文件、读取小型README并校验哈希。反向检查：不能进入原始数据目录，不能读取未交付文件，不能在交付目录新建文件、覆盖文件或删除文件，也不能沿软链接跳出批准范围。测试结束后撤销临时账号或加入生产访问组前先复核目录权限。

只读并不等于禁止复制。合作者如果能读取数据，通常可以保存副本。因此交付前要决定文件本身是否可以下载；如果只能在受控环境查看，应考虑在服务器上提供受限会话、脱敏数据或汇总结果，而不是把下载权限误称为只读。任何截图、

图表也可能含样本编号或临床字段，需按相同规则检查。审计时保留命令、测试账号、时间、目录清单和预期结果，避免只保存一张“权限截图”。

示例：在临时目录演练 ACL，不要直接改生产目录

下面只在新建的临时目录演示检查步骤。执行前由管理员确认 setfacl/getfacl 可用、文件系统支持ACL，并将变量改为专用测试路径；不要照搬到共享根目录。演练要验证默认ACL是否影响新建文件、目录的执行权限是否允许遍历，以及mask是否让实际有效权限低于配置值。输出的用户名和路径应脱敏后再分享。

```
set -eu
umask 077
TEST_DIR="${TMPDIR:-/tmp}/readonly-share-demo-$$"
mkdir -m 700 "$TEST_DIR"
mkdir "$TEST_DIR/project-copy"
printf 'synthetic demo only\n' > "$TEST_DIR/project-copy/README.txt"
# Replace reviewer with a dedicated temporary account after admin approval.
getfacl -p "$TEST_DIR" "$TEST_DIR/project-copy" "$TEST_DIR/project-copy/README.txt"
# Apply ACL only to this disposable demo path, then inspect effective rights.
setfacl -m u:reviewer:--x "$TEST_DIR"
setfacl -m u:reviewer:r-x "$TEST_DIR/project-copy"
setfacl -m u:reviewer:r-- "$TEST_DIR/project-copy/README.txt"
getfacl -p "$TEST_DIR" "$TEST_DIR/project-copy" "$TEST_DIR/project-copy/README.txt"
# Login as reviewer in a separate session and verify read succeeds, write fails.
```

命令中的 reviewer 只是占位账号，不能作为真实账号照抄。生产方案应由系统管理员审核身份、组关系和退出流程。测试账号可以用 cat 验证读取，并尝试在临时副本创建文件以确认被拒绝；不要通过删除真实文件来证明权限。撤销时既要移除命名ACL，也要清查组成员、默认ACL、软链接和共享挂载。遇到 ACL 与容器挂载叠加时，分别从宿主机和容器内验证。

交付后还要有撤销和复核记录

访问期限到期时，应撤销账号或ACL，检查已挂载的共享目录，并记录执行人和完成时间。如果合作延期，重新确认项目负责人仍同意共享范围，而不是自动延长。每次新增文件、替换结果或改变目录结构都要重跑权限测试，因为新文件可能继承不同的默认权限。项目结束后按数据管理计划决定保留、归档或删除副本，不要承诺“撤销后对方无法保留已下载文件”。

真正可靠的交付是“指定人、指定副本、指定期限、指定用途、可验证访问结果”的组合。权限最小化能降低误操作风险，但不能取代合作协议、伦理审批、备份和数据脱敏。若团队没有统一账号或无法实现目录隔离，应先由管理员评估账号与存储方案，再开放任何外部访问。

权限变更用最小化的回滚演练验证

正式开放之前，管理员应先在一个隔离的演练目录中复制相同的目录层级、组关系、默认ACL和容器挂载配置。只模拟目录树结构和虚拟文件名，不要把真实样本复制到演练区。邀请一个权限与生产账号相同、但只含少量合成文件的测试账号，依次执行列目录、读取文件、写入文件、删除文件、访问父目录和跟随链接等操作。把每个操作的预期结果和实际退出码记录下来。如果环境使用NFS、SMB或对象存储，权限映射行为可能与本地ext4不同，必须在实际存储后端上验证，不能把本机测试结果当作远端证据。

ACL变更需要有回滚方案。记录变更前的getfacl输出、目标账号、修改命令和责任人；演练撤销时确认命名用户ACL、组ACL和默认ACL都已移除，并在账号重新登录后复测。目录默认ACL会影响之后新建的文件和子目录，因此仅修改当前已有文件并不代表未来交付内容也保持正确。遇到“权限看起来正确但访问仍被拒绝”时，依次检查路径上每一级目录的执行权限、ACL mask、父目录继承、挂载参数、容器用户映射和服务端缓存。避免简单把目录改成777，这会同时扩大写权限和信息暴露范围。

如对方只需要查看一份报告，可以考虑导出脱敏PDF或HTML并通过受控渠道交付，而不是授予服务器账号。需要反复查看多个文件时，建立独立的结果副本和只读查看角色更便于审计。任何共享链接都要设置访问期限和撤销责任人；链接被撤销无法抹去对方此前已下载的副本，所以交付前仍须确认数据授权和去标识情况。因合作范围变化新增文件时，应重走

审批和验收，不要直接把文件写进已开放目录。

最后形成一份可以交接的访问记录：接收账号、项目授权来源、开放目录、文件清单摘要、访问起止时间、正反测试结果、管理员和撤销日期。项目负责人应确认内容与合作约定一致，系统管理员确认权限生效，数据负责人确认脱敏和共享边界。三方责任不应由一句“已设置只读”替代。本文示例命令并不代表已在某个特定服务器或存储系统测试，部署前按操作系统和文件系统版本复核工具行为。

边界变化时的审批和撤销流程

如果合作人新增、目录扩展或合作目的变化，访问权限应重新确认。可以把“申请—批准—配置—双向测试—开放—到期撤销—留痕”做成一个短流程。申请人写明研究目的和所需文件类型，项目负责人确认共享范围，数据管理人核对协议与脱敏要求，管理员执行最小权限配置，接收者完成普通账号测试。角色分工能避免由一个人同时判断数据是否可共享、配置权限并自证权限正确。若需要紧急交付，也应保留批准记录和到期时间，不能用临时账号长期开放。

撤销前先确认接收方不再需要正在运行的只读会话，随后移除用户或项目组授权、终止会话、清理外部共享链接并检查权限继承。记录撤销后的负向测试结果。若底层服务使用缓存或挂载点，权限撤销可能不会立即体现在已存在的进程中，管理员应核对实际系统行为。对合作方已下载的文件，技术撤权无法收回其副本；因此共享批准、文件水印或去标识以及合作协议都应在开放前完成。

一个容易忽略的风险是结果文件元数据和隐藏内容。Excel可能保留批注、筛选表和隐藏列，PDF可能包含可复制的文本层，图表可能带有原始样本标签。交付前应检查文件本身，而不仅仅是文件名。使用复制出来的交付目录能把审查对象限定在一份快照；生成清单后再计算哈希，保证验收时对应的是同一批文件。任何后续修改都产生新版本和新摘要，避免接收方看到内容不一致却无法追溯。

不要把“外部合作者”当成单一角色

联合研究中可能同时存在外校PI、统计顾问、测序服务人员和短期实习人员，他们需要的文件和保密责任并不相同。访问矩阵应记录角色对应的研究目的，而不是仅记录单位名称。统计顾问可能需要去标识化矩阵和分析说明，测序人员只需要原始测序文件的交接清单，PI可能只需要汇总图表。将所有外部人员放进一个共享组，会让权限范围随着项目变化而失控。人员名单发生变动时，先确认原账号是否仍有效，再新增新账号，不要把旧账号改名转给新人。

跨机构共享还可能受到协议、伦理审批、数据出境或机构信息安全制度约束。服务器目录权限只能控制某一存储系统中的读写，不会自动满足这些要求。由项目负责人确认可以分享的内容，技术人员按批准清单实施。若权限目标无法在现有系统实现，例如只能开放父目录却无法隐藏兄弟目录，应停止配置并重新设计交付结构，而不是先开放再观察是否有人误读。

对无须长期在线查看的结果，可在批准后生成单次交付快照，并把快照摘要发送给接收方。接收方完成校验后，服务器端临时副本按约定归档或删除。若结果需要持续协作，建立项目级账号、到期策略和访问复核日期。两种方式都应保留交付版本，便于后来确认双方看到的是哪份文件。只读共享降低误删风险，但不能保证接收方理解结果，也不能替代研究团队对统计方法和结论的复核。

配套练习包

本PDF对应的ZIP包含本文代码、主题模板或合成数据、README和SHA256校验文件。运行前核对包内清单，并按文章说明在独立目录验证。

参考资料

Linux setfacl 手册 · 来源资料

Docker bind mount 文档 · 来源资料

数据保护原则指南 · 来源资料

操作建议：先在合成小样本上验证流程，再依据项目参考、标签合同、存储策略与获配资源验收真实数据。