



链滴

NFS 共享存储快速搭建

作者: [etscript](#)

原文链接: <https://ld246.com/article/1563353169822>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

- [共享存储可以有多种实现的方式，项目No.1用nfs提供共享存储服务]

master or slave or anywhere

安装nfs server包

```
apt-get install nfs-kernel-server
```

配置nfs server

```
vim /etc/exports
```

```
# 将远程访问的所有普通用户及所属组都映射为匿名用户或用户组 (nfsnobody)
# 允许客户端从大于1024的tcp/ip端口连接服务器
# 这种可以用于挂载者不对存储修改权限，多app访问时也不会出现权限问题
/data/project *(rw,all_squash,insecure)
```

```
# 将数据同步写入内存缓冲区与磁盘中，效率低，但可以保证数据的一致性
# 不将root用户及所属组都映射为匿名用户或用户组（默认设置）
# 这里这么配置，主要是k8s中创建pvc时会修改文件用户
/data/sys_data *(rw,sync,no_root_squash)
```

启动nfs server

```
service nfs-kernel-server restart
```

nfs详细的配置参数

其实漏洞形成的原理就是权限不对，`/etc/exports`这个文件中的权限设置。

`/etc/exports` 文件格式

<输出目录> [客户端1 选项（访问权限,用户映射,其他）] [客户端2 选项（访问权限,用户映射,其他）]

a. 输出目录：输出目录是指NFS系统中需要共享给客户机使用的目录；

b. 客户端：客户端是指网络中可以访问这个NFS输出目录的计算机

指定ip地址的主机：`192.168.0.200`

指定子网中的所有主机：`192.168.0.0/24 192.168.0.0/255.255.255.0`

指定域名的主机：`david.bsmart.cn`

指定域中的所有主机：`*.bsmart.cn`

所有主机：`*`

c. 选项：选项用来设置输出目录的访问权限、用户映射等。

设置输出目录只读：`ro`

设置输出目录读写：`rw`

d. 用户映射选项

`all_squash`：将远程访问的所有普通用户及所属组都映射为匿名用户或用户组（`nfsnobody`）；

`no_all_squash`：与`all_squash`取反（默认设置）；

`root_squash`：将`root`用户及所属组都映射为匿名用户或用户组（默认设置）；

`no_root_squash`：与`rootsquash`取反；

`anonuid=xxx`：将远程访问的所有用户都映射为匿名用户，并指定该用户为本地用户（`UID=xxx`）；

`anongid=xxx`：将远程访问的所有用户组都映射为匿名用户组账户，并指定该匿名用户组账户为本用户组账户（`GID=xxx`）；

e. 其它选项

`secure`：限制客户端只能从小于`1024`的`tcp/ip`端口连接`nfs`服务器（默认设置）；

`insecure`：允许客户端从大于`1024`的`tcp/ip`端口连接服务器；

`sync`：将数据同步写入内存缓冲区与磁盘中，效率低，但可以保证数据的一致性；

`async`：将数据先保存在内存缓冲区中，必要时才写入磁盘；

`wdelay`：检查是否有相关的写操作，如果有则将这些写操作一起执行，这样可以提高效率（默认设置）；

`no_wdelay`：若有写操作则立即执行，应与`sync`配合使用；

`subtree`：若输出目录是一个子目录，则`nfs`服务器将检查其父目录的权限(默认设置)；

`no_subtree`：即使输出目录是一个子目录，`nfs`服务器也不检查其父目录的权限，这样可以提高效率。

文中参考引用文章（链接若失效请留言）

[# NFS配置不当那些事](#)