服务器设置禁止直接访问目录或文件,可以避免服务器文件直接暴露,导致平台信息泄露。以下是Nginx[Apache]IIS的配置方法:

Nginx

- 1. 修改 Nginx 的配置文件□linux可通过命令: find / -name nginx.conf 来查找配置文件路径。
- 2. 在 http 块下添加以下配置代码:

```
location /Logs/ {
return 403;
```

如宝塔:

}

```
站点修改[
            ] -- 添加时间[2022-05-30 10:12:05]
域名管理
            提示: Ctrl+F 搜索关键字, Ctrl+S 保存, Ctrl+H 查找替换
子目录绑定
               52
                  location ~ .*\.(gif|jpg|jpeg|png|bmp|swf)$
               53
网站目录
               54
                  expires
                                  30d;
                   error_log /dev/null;
               55
访问限制
               56
                  access_log /dev/null;
               57
               58
流量限制
               59
                   location ~ .*\.(js|css)?$
               60
伪静态
               61
                     expires
                                  12h;
               62
                     error_log /dev/null;
默认文档
               63
                      access_log /dev/null;
               64
配置文件
               65
                     location /Logs/ {
               66
               67
                     return 403;
SSL
               68
               69
PHP版本
               70
                     access_log /www/wwwlogs
               71
                     error_log /www/wwwlogs/ error.log;
Composer
               72 }
Tomcat
              保存
重定向
            此处为站点主配置文件,若您不了解配置规则,请勿随意修改.
反向代理
```

- 3. 保存并关闭文件。
- 4. 使用命令nginx -s reload 重载Nginx配置,使配置生效。

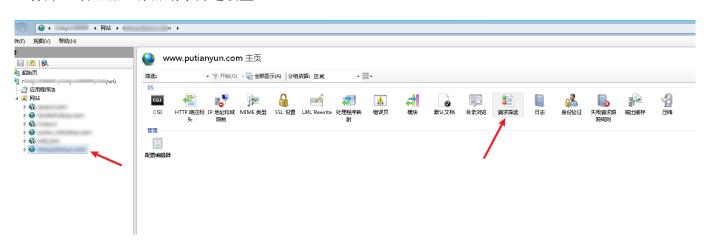
Apache

1. 修改Apache 的配置文件□ httpd.conf

- 2. 加入以下配置代码
- <Location /Logs/>
 Order allow,deny
 Deny from all
- </Location>
- 3. 保存并关闭文件。
- 4. 重启httpd服务。

IIS

1. 打开IIS管理器,添加请求筛选设置



2.URL模块添加【拒绝序列】



	拒绝序列	? X
URL 序列(U): /Logs/		
	确定	取消

■ 重启IIS