1. 统计文件夹数量 ls -l | grep "^d" | wc -l
2. 查看端口占用 netstat -pan | grep 8080
3. 查看文件行数 awk '{print NR}' git-clone-commands.sh | tail -n 1
4. 显示前10个文件 ls | head -n 10
5. 后台运行, 把标准错误和标准输出同时输出到指定的日志文件， nohup java -jar \*\*\*\*.jar > git-repo-dependency-tree-check.log 2>&1 &
6. 执行结果输出到console同时输出到文件 ./check-dependency-tree.sh | tee ./script\_log/check-dependency-tree.log
7. 取出<=后面的数字 cat get-dependency-tree-2500-end.sh | grep "$start <= " | cut -d "=" -f 2 | cut -d ")" -f 1
8. 替换文件中的字符并写回 sed -i 's/<= "+lastRepoNum+"/<= "+gitRepoNum+"/g' get-dependency-tree-2500-end.sh
9. 切换到root用户 sudo su - (sudo –i 如果security设置了的话)
10. 显示隐藏文件 ls -al
11. 后台运行 nohup ./sh/get-dependency-tree-1-99.sh > /opt/data/log/get-dependency-tree-1-99.log 2>&1 &
12. 用于查询DNS的记录，查看域名解析是否正常 nslookup
13. sz 文件名 发送文件到本地
14. rz 上传本地文件到服务器
15. <https://cloud.tencent.com/developer/article/1722345> 清空文件夹下文件
16. find ./ “\*-latest” | wc -l 查找当前目录下的指定目录数
17. ls -d \*-latest | wc -l 查找当前目录下的指定目录数
18. 使用域名的都要通过DNS解析，优先级最高的是本地hosts文件里配置，/etc/hosts,hosts没有就找/etc/resolv.conf,

内容如下

search cn.prod

options rotate timeout:1 attempts:3

nameserver 10.67.230.8

#nameserver 10.29.4.100

nameserver 10.26.42.201

其中有slave节点，有master节点，添加新域名先在master里添加，在同步到slave

1. nslookup 域名 [DNS IP] 可以查看解析出来的ip ，通过 所选的DNS IP
2. 查看vm上的定时任务 crontab -l

0 0 \* \* 0 systemctl restart salt-minion >/dev/null 2>&1

#5 5,13,21 \* \* \* /opt/dns\_check/dns\_check.sh

0 2 \* \* \* gitlab-rake gitlab:backup:create

1. cat /opt/dns\_check/dns\_check.sh

#!/bin/bash

cat << EOF > /etc/resolv.conf

search cn.prod

options rotate timeout:1 attempts:3

EOF

echo "nameserver 10.67.230.8" >> /etc/resolv.conf

echo "nameserver 10.29.4.100" >> /etc/resolv.confPROD

1. cat /etc/resolv.conf

search cn.prod

options rotate timeout:1 attempts:3

nameserver 10.25.9.21

nameserver 10.25.9.22

nameserver 10.26.42.201

1. power dns 服务器 可以解析外网
2. df -u 查看硬盘
3. /etc/keepalived/keepalived.conf 虚ip设置 重启 keepalived：systemctl restart keepalived
4. 修改nginx 配置： portal上 /usr/local/nginx/conf.d/upstream.conf 把后端ip改了，重新加载nginx：/usr/local/nginx/sbin/nginx -t，/usr/local/nginx/sbin/nginx -s reload

nginx config

$ nginx -s reload 软重启

$ cd /etc/nginx/ssl 证书路径，key用pem文件直接改名得到，后缀用.pem

$ cat /etc/nginx/conf.d/nexus.conf nginx代理nexus的配置

如果部署在docker，暴露的是80端口，http协议，不需要证书