jumperserver：ansible-172-25-5-68主机通过ansible远程批量操作

把机器所有的权限都改成21ops.com@#M

ansible -i guozhichao gzc -m shell -a 'echo "root:21ops.com@#M" |chpasswd'

东莞和香港的都加上黑白名单允许172.25.5.68和 172.24.2.248访问

cat /tmp/hosts.allow

# /etc/hosts.allow: list of hosts that are allowed to access the system.

# See the manual pages hosts\_access(5) and hosts\_options(5).

#

# Example: ALL: LOCAL @some\_netgroup

# ALL: .foobar.edu EXCEPT terminalserver.foobar.edu

#

# If you're going to protect the portmapper use the name "rpcbind" for the

# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.

#

sshd: 172.25.5.68,172.24.2.248

cat /tmp/hosts.deny

# /etc/hosts.deny: list of hosts that are \_not\_ allowed to access the system.

# See the manual pages hosts\_access(5) and hosts\_options(5).

#

# Example: ALL: some.host.name, .some.domain

# ALL EXCEPT in.fingerd: other.host.name, .other.domain

#

# If you're going to protect the portmapper use the name "rpcbind" for the

# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.

#

# The PARANOID wildcard matches any host whose name does not match its

# address.

#

# You may wish to enable this to ensure any programs that don't

# validate looked up hostnames still leave understandable logs. In past

# versions of Debian this has been the default.

# ALL: PARANOID

sshd: ALL

ansible -i guozhichao gzc -m copy -a 'src=/tmp/hosts.allow dest=/etc/hosts.allow backup=yes'  
ansible -i guozhichao gzc -m copy -a 'src=/tmp/hosts.deny dest=/etc/hosts.deny backup=yes'

验证配置是否更改

ansible -i guozhichao gzc -m shell -a "sed -n '/^[^#]/p' /etc/hosts.allow"

ansible -i guozhichao gzc -m shell -a "sed -n '/^[^#]/p' /etc/hosts.deny"

更改后不需要重启sshd服务，立刻就生效