## 初始设定规定

规定主机初始设定

比如阿里云服务器申请的时候应当规定 密码还是密钥登录，安全组设置，系统使用哪个版本的系统，打标签规定，镜像规定等

对象是运维

运维为了统一管理方便，一般倾向于将密码设成一样的或使用同一个KEY。如果泄露的话有很大风险。还有可能某主机用ssh key的方式与其他主机都设成免密连接。

安全组设置，应当设置SSH登录端口只能jumpserver 的IP才能访问。

这样能保证主机只能从jump server登录，无法直接登录，保证所有操作记录都在jump server，可保证审计到所有主机操作。

至于黑客留的网马后门，通过这个执行的命令。归属于应用安全部分。需要日志审计发现。

## 主机初始化规定

使用基础镜像，符合安全基线的镜像生成服务器。

K8S使用安全镜像仓库生成容器。

## 管理方式规定

必须使用jump server管理，不允许直接登录。Jumpserver支持K8S。

## 操作规定

规定服务器只能通过jumpserver登录，

规定批量命名只能通过jumpserver执行。

## 权限申请规定

应当有申请系统，申请系统串联 SDL工作流，申请人在申请系统向运维提出权限申请，申请系统串联到SDL工作系统，申请人在SDL进行权限备案，项目进度备案，进行安全开发培训，（内容可加入服务器安全使用），考试通过后，SDL向运维发出信号，运维可进行权限分配。

## 权限消除

OA系统应当与 IAM，或其他系统管理。员工离职后，删除员工账户，回收权限。

## 审计规定

Jumpserver可通过接口的方式将所有操作记录拉下来，多个junpserver的记录可以这样汇总到一起进行 审计。