防范勒索病毒操作文档(windows 版)

一、 基础环境

阿里云上客户，确认已经完成 OSS 和云安全中心产品采购。

二、 提前做好快照备份

三、 安全配置

先装云安全中心，进行云安全中心的配置，针对勒索病毒攻击途径，进行防护

攻击途径：

1. 操作系统漏洞
2. 应用服务漏洞（Web-CMS 漏洞）
3. 操作系统弱口令
4. 远程登录协议 RDP 暴力破解
5. 网络共享端口访问

漏洞修复：在漏洞管理里面配置相关的规则。然后进行漏洞扫描，扫描处漏洞之后。选择性进行修复。（Windows 漏洞一键扫描，扫描结果出来，检测漏洞，按照漏洞威胁等级进行修复。优先选择高危漏洞修复，中危漏洞，低危漏洞自己查看，如果没有危害，可以忽略，但不要添加白名单。）

安全告警设置：规则配置，配置常登陆 ip（本公司公网 ip），常登陆地点（本公司地点），防暴力破解规则建议 5 分钟内登陆 5 次失败封 6 个小时。

主动病毒查杀：开启添加需要管理的服务器。选择自己需要管理的服务器。

网站后门查杀：开启添加需要管理的服务器。

客户端自保护：开启添加需要管理的服务器。

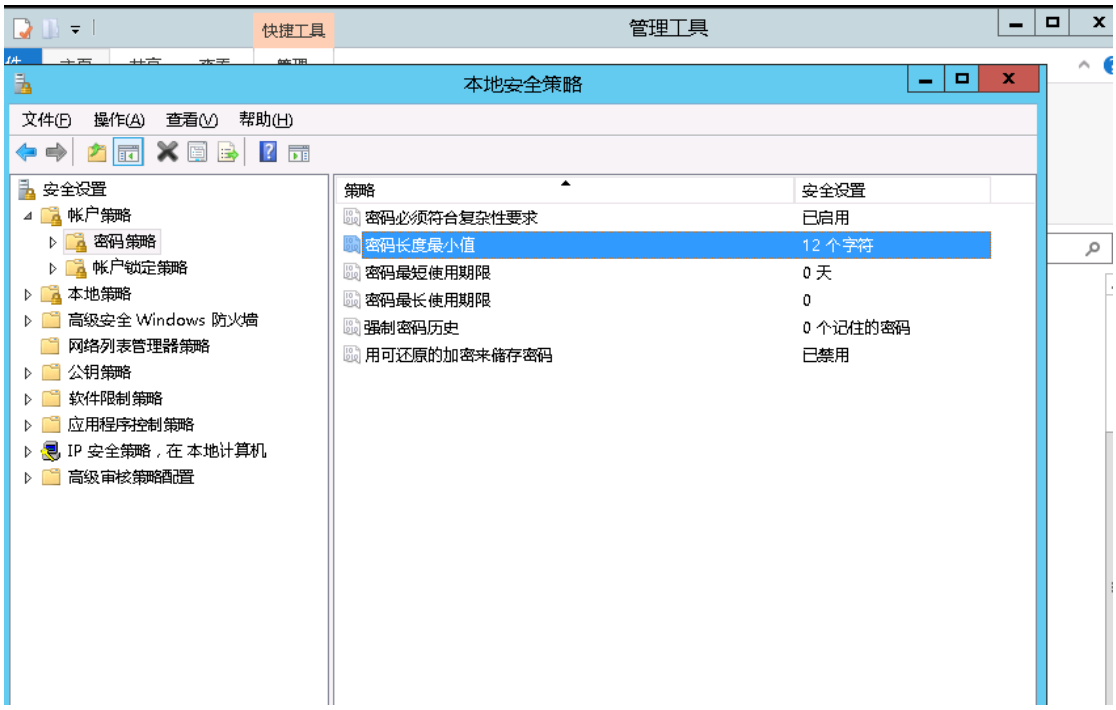
报警通知：漏洞、安全告警、云平台配置检测、应急漏洞情报。（添加接收联系人）

共享端口禁用或限制人员：安全组规则配置。新建一条安全组，入方向禁止其他所有端口， 远程 3389 tcp80 443 icmp （根据业务需求，可以动态调整）

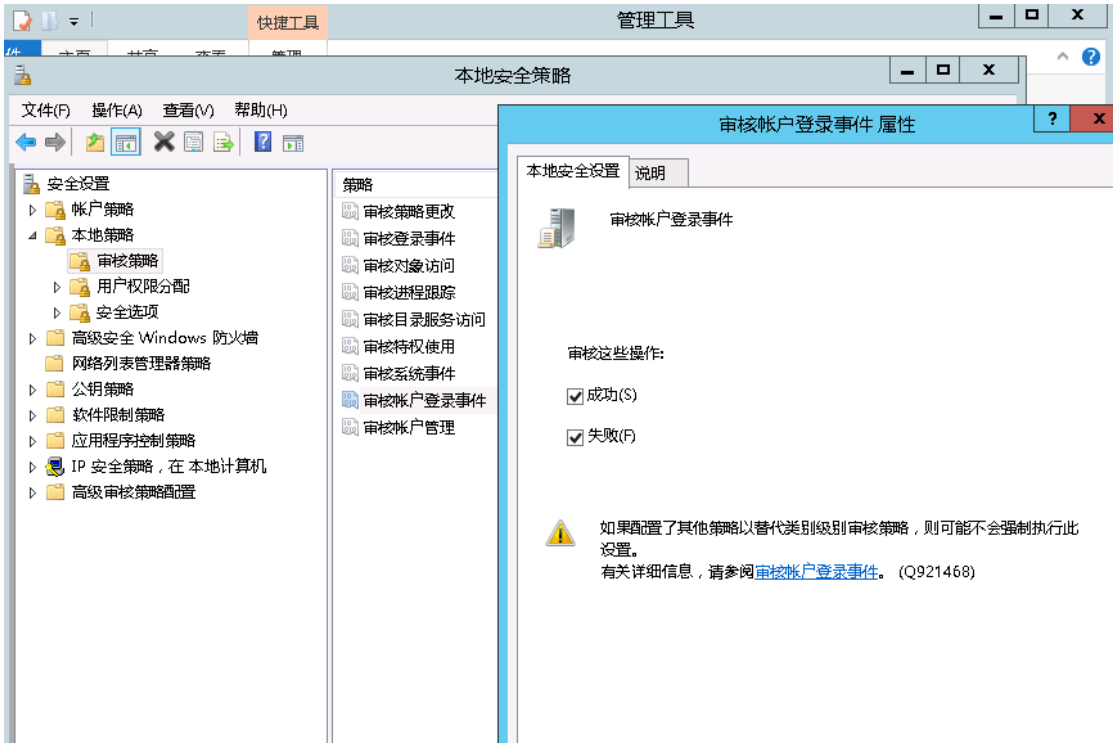
四、　基线配置

基线配置：系统弱口令，windows 基线加固配置（建议如下）

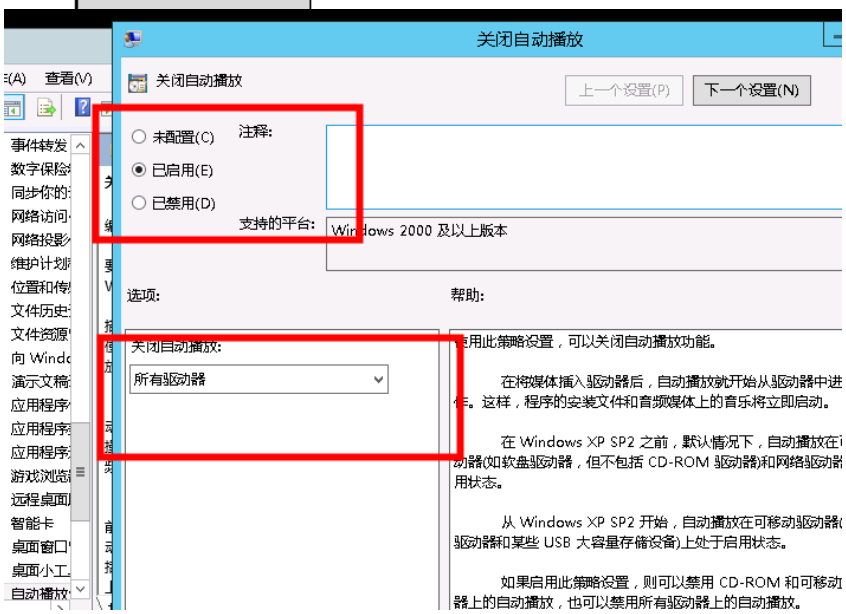
配置要求内容	1、最短密码长度 12 个字符； 2、启用本机组策略中密码必须符合复杂性要求的策略，即密码至少包含以下四种类别的字符中的三种： 英语大写字母 A, B, C, ... Z 英语小写字母 a, b, c, ... z 西方阿拉伯数字 0, 1, 2, ... 9 非字母数字字符，如标点符号，@, #, $, %, &, *等
操作方法	参考配置操作 1、"管理工具->本地安全策略->帐户策略->密码策略->密码长度最小值->属性" 2、"管理工具->本地安全策略->帐户策略->密码策略->密码必须符合复杂性要求->属性"
检查方法	1、检查最小值设置，大于等于 12 为符合要求； 2、检查单选框"已启动"状态，选中"已启动"为符合。



容	
操作方法	**参考配置操作** "管理工具->本地安全策略->审核策略->审核登录事件->属性"。 **参考配置操作** "控制面板->管理工具->本地安全策略->审核策略->审核登录事件->属性"。



操作方法	**参考配置操作** 点击开始→运行→输入 gpedit.msc，打开组策略编辑器，浏览到计算机配置→管理模板→系统” **参考配置操作** 点击开始->运行→输入 gpedit.msc，打开组策略编辑器，浏览到计算机配置->管理模板->Windows 组件->自动播放策略”



修改系统登录密码，并重新启动系统，让修改配置生效。