CiscoACS替代方案系列之二(Splunk)Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/583/2021_2022_CiscoACS_E6_9B_c101_583975.htm Cisco的ACS服务器可以提供完善AAA服务，包括认证、授权和记账的功能。但价格较高，不适合中小企业使用。其实我们可以让Cisco网络设备本身记录配置的变更，并将变更的内容发送到syslog服务器上，然后由syslog定时将相关的记录过滤出来，通过邮件发送到指定的邮箱来实现记账的功能。 在这里我使用Splunk作为syslog服务器，splunk是linux下一款优秀的日志收集和分析软件，免费版可以提供每天500M的日志索引量，对于中小企业已经足够了。下面我们以cisco的交换机和防火墙为例： 1）cisco交换机配置 archive log config logging enable logging size 200 hidekeys notify syslog logging trap notifications logging x.x.x.x 2） cisco ASA5500配置 logging enable logging host inside x.x.x.x logging class config trap notifications 3）splunk基本配置 linux下splunk的安装具体见www.splunk.com，同时需要安装smtp邮件系统，我使用的是postfix。安装完成后通过IE访问splunk管理页面。在admin页面中定义使用udp 514端口接受syslog日志。 4）splunk报警配置 在搜索框中输入以下条件，并点击搜索框左边的小箭头，选择‘ save search ’。 %ASA-5-111008 OR %PARSER-5-CFGLOG_LOGGEDCMD startminutesago=60 在‘ save search ’的定义页面中选择以下选项， 选中 Run this search on a schedule schedule：run every hour alert：alert when number of event greater than 1 send email : xxx@xxx.com 选中 include results 5）验证邮件报警功能 在交换机或者防火墙上修

改配置，splunk将每隔60分钟搜寻一下前60分钟收到的日志，将与配置变更有关的内容自动发送到你指定的邮箱中，邮件范例如下： From: splunk@localhost To: xxx@xxx.com Content ：Saved search results. Name: Config Change Query Terms: now=1242100800 %ASA-5-111008 OR %PARSER-5-CFGLOG_LOGGEDCMD startminutesago=60 Alert was triggered because of: Saved Search [Config Change]: number of events(16) greater than 1 Search results attached: attachment: %PARSER-5-CFGLOG_LOGGEDCMD: User:xxx logged command:service timestamps log datetime 