**服务器网络安全维护指南**

一．巡检

定期对服务器、网络安全、系统性能的检查。每台服务器、网络设备及安全设备至少保证每周检查两次，每次检查的结果要求进行登记记录。

二．数据备份

用于在块设备级别 (block device level) 上进行硬盘的备份与恢复（包括系统盘和数据盘），现有服务器采用的是青云全备加增量备份的方式进行备份策略。每次更改配置、策略后，都要及时更新备份文件，保证当前为备份最新数据。

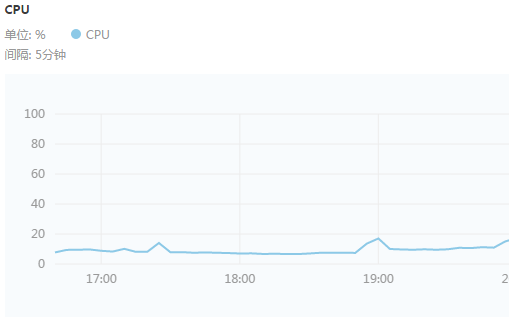
* 数据备份
  + 块设备级别的备份与恢复
  + 捕捉硬盘在某一个时刻的状态，未来可以随时恢复到这个状态
  + 可以同时对多张硬盘做备份，也可以对正在运行的主机做在线备份
* 备份链
  + 每条备份链包括一个全量备份点以及多个增量备份点
  + 每次做全量备份都会产生一个新的备份链



三． 监控及设置告警策略

云服务器、网络及防火墙策略的监控工作。每天正常工作期间必须保证监视所有服务器、网络流量及安全情况状态，一旦发现服务器、网络流量或安全防掮异常，要及时采取相应措施。

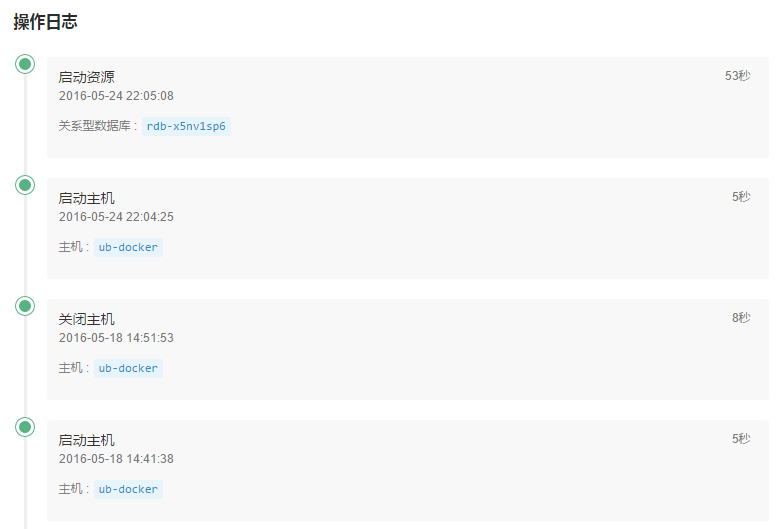
* + CPU 利用率 / 内存利用率 / 磁盘使用量 / 网络流量





四． 日志

服务器、网络设备及安全设备的相关日志操作。每台服务器、网络设备及安全设备保证每周或依据数据情况对相关日志进行整理，整理前对应的各项日志如应用程序日志、安全日志、系统日志等应进行保存。





五． 防火墙及端口转发

根据应用需要对相应的端口进行开放。默认是拒绝所有端口。

目前业务采用的是标准HTTP协议，非80端口的端口转发方式。没有使用到ssl,tls等安全协议。





六． 登陆安全

1. 采用青云平台二次登录验证和失败告警。
2. 云服务器采用OPEN-VPN证书方式进行远程连接青云上的私有网络。没有使用到 SSL、TLS、IPSec、Telnet、SSH等等相关协议。



七．不定时的相关工作

每台服务器如有应用软件更改、需要安装新的应用程序或卸载应用程序等操作，应提前告知所有管理员。

密码定期更改工作。每台服务器、网络设备及安全设备保证至少每一个月更改一次密码，密码长度不少于8位，且要满足复杂度要求。

八． 杀毒

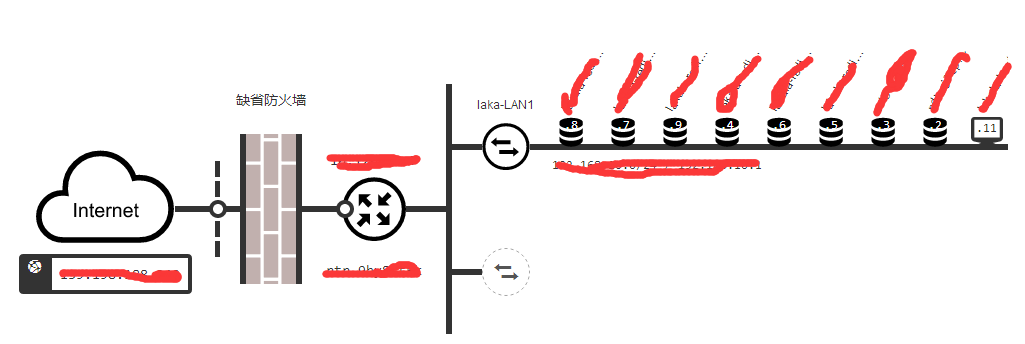
采用的是云模式下无代理杀毒。

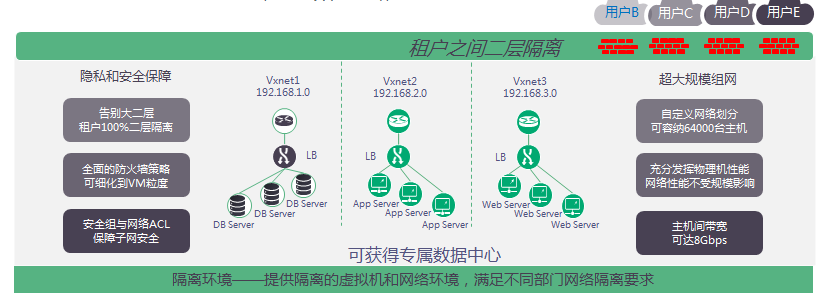
系统管理人员要定时对系统服务器进行病毒检查，发现病毒要及时处理。



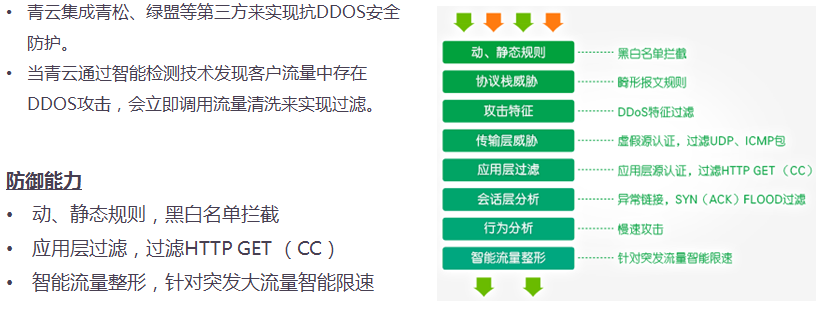
九． 网络拓扑及协议

网络采用是青云私有VPC网络，100%二层网络隔离，防止数据泄露.





十． 抗DDOS服务



十一 云平台上的账号角色与权限分配

