UCan下午茶

公有云安全运维实践谈

绿盟科技
侯奎宇

UCLOUD

容易忽略什么？

安全责任边界

云平台安全 ≠ 租户安全

等保2.0

对 GB/T 22239-2008 的修订完成后，基本要求标准成为由多个部分组成的系列标准，目前主要有六个部分：

——GB/T22239.1-XXXX 信息安全技术 网络安全等级保护基本要求
第 1 部分 安全通用要求；

——GB/T 22239.2-XXXX 信息安全技术 网络安全等级保护基本要求
第 2 部分 云计算安全扩展要求；

——GB/T 22239.3-XXXX 信息安全技术 网络安全等级保护基本要求
第 3 部分 移动互联安全扩展要求；

——GB/T 22239.4-XXXX 信息安全技术 网络安全等级保护基本要求
第 4 部分 物联网安全扩展要求；

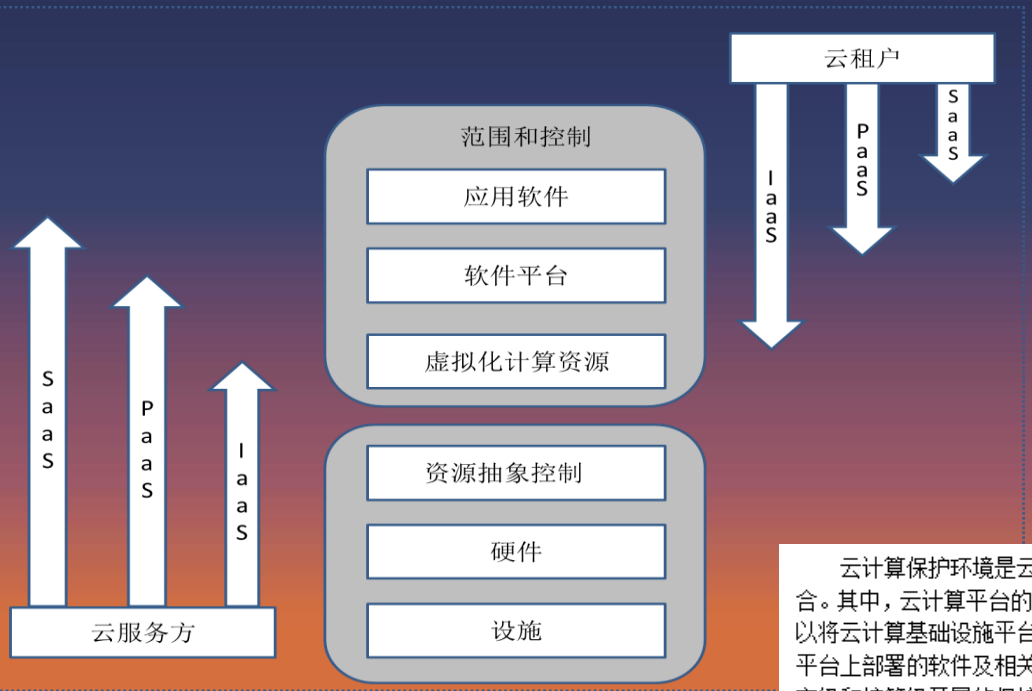
——GB/T 22239.5-XXXX 信息安全技术 网络安全等级保护基本要求
第 5 部分 工业控制安全扩展要求。

——GB/T 22239.6-XXXX 信息安全技术 网络安全等级保护基本要求
第 6 部分 大数据安全扩展要求。

租户

云平台（CSP）

等保2.0



云计算保护环境是云服务方的云计算平台，及云租户在云计算平台之上部署的软件及相关组件的集合。其中，云计算平台的等级保护定级和按照等级的保护工作由云服务方负责，对于大型云计算平台可以将云计算基础设施平台及辅助支撑系统划分为不同的等级对象，各自独立定级。如果云租户在云计算平台上部署的软件及相关组件可以构成等级保护定级对象，则一般称为云租户信息系统，针对其的具体定级和按等级开展的保护工作由云租户负责。

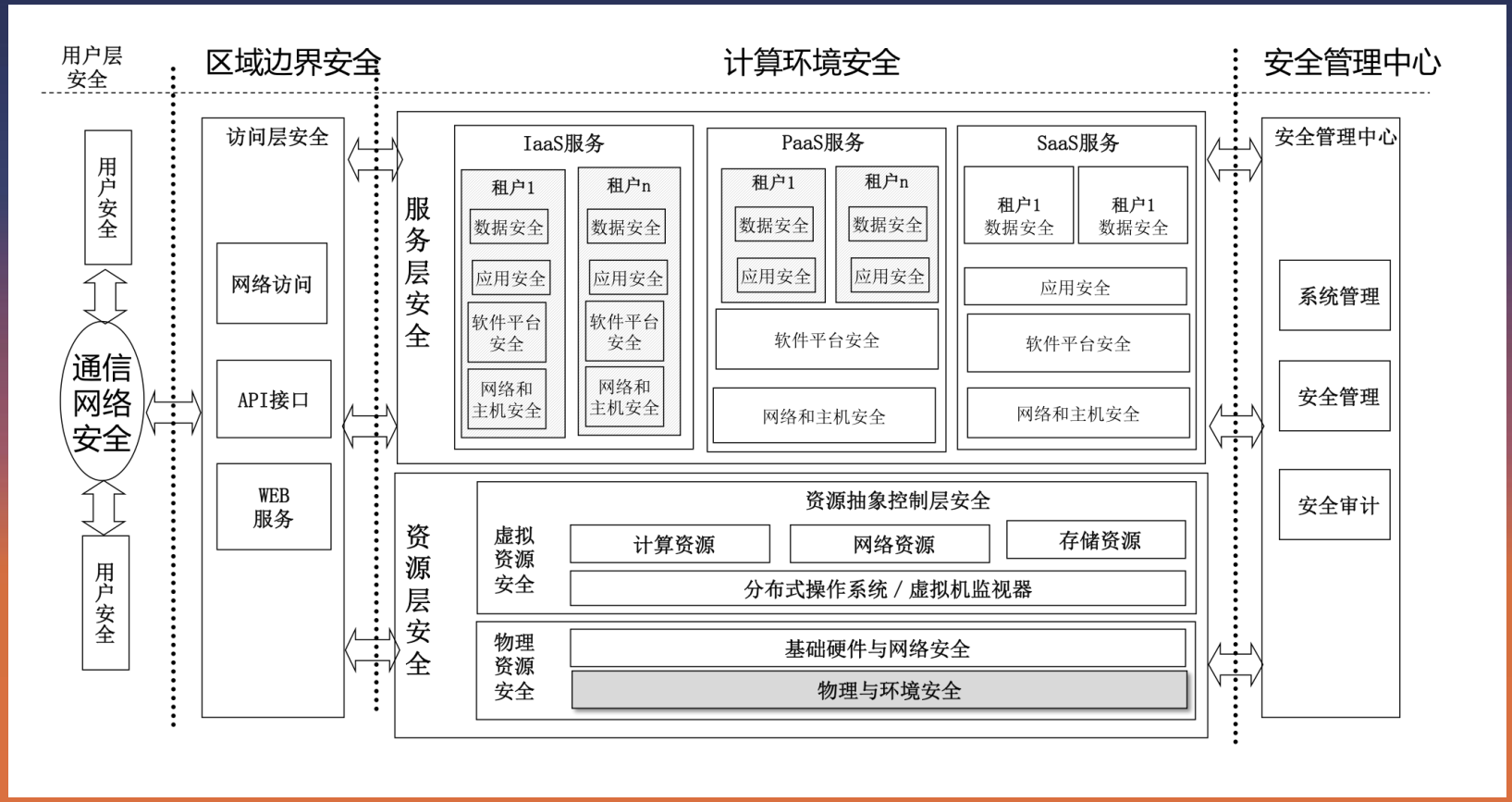
云服务方的云计算平台可以承载多个不同等级的云租户信息系统，云计算平台的安全保护等级应不低于其承载云租户信息系统的最高安全保护等级，并且云计算平台的安全保护等级应不低于第二级，因此本分部的安全设计技术要求从第二级开始。

等保2.0

表C.1　IaaS 模式下云服务方与云租户的责任划分

层面	安全要求	安全组件	责任主体
物理和环境安全	物理位置选择	数据中心及物理设施	云服务方
网络和通信安全	网络结构、访问控制、远程访问、入侵防范、安全审计	物理网络及附属设备、虚拟网络管理平台	云服务方
		云租户虚拟网络安全域	云租户
设备和计算安全	身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、镜像和快照保护	物理网络及附属设备、虚拟网络管理平台、物理宿主机及附属设备、虚拟机管理平台、镜像等	云服务方
		云租户虚拟网络设备、虚拟安全设备、虚拟机等	云租户
应用和数据安全	安全审计、资源控制、接口安全、数据完整性、数据保密性、数据备份恢复	云管理平台（含运维和运营）、镜像、快照等	云服务方
		云租户应用系统及相关软件组件、云租户应用系统配置、云租户业务相关数据等	云租户

等保2.0


用户层安全
区域边界安全
计算环境安全
安全管理中心
用户安全
通信网络安全
用户安全
访问层安全
网络访问
API接口
WEB服务
服务层安全
IaaS服务
租户1
数据安全
应用安全
软件平台安全
网络和主机安全
租户n
数据安全
应用安全
软件平台安全
网络和主机安全
PaaS服务
租户1
数据安全
应用安全
租户n
数据安全
应用安全
软件平台安全
网络和主机安全
SaaS服务
租户1 数据安全
租户1 数据安全
应用安全
软件平台安全
网络和主机安全
资源层安全
资源抽象控制层安全
虚拟资源安全
计算资源
网络资源
存储资源
分布式操作系统 / 虚拟机监视器
物理资源安全
基础硬件与网络安全
物理与环境安全
安全管理中心
系统管理
安全管理
安全审计

安全合规的架构体系

- 物理及环境安全
- 合规性
- 访问控制
- 网络安全
- 审计和跟踪
- 数据安全
- 事故和风险管理

- 物理及环境安全
- 网络和通信安全
- 设备和计算安全
- 应用和数据安全
- 安全管理机构和人员
- 系统安全建设管理
- 系统安全运维管理

怎么开始？

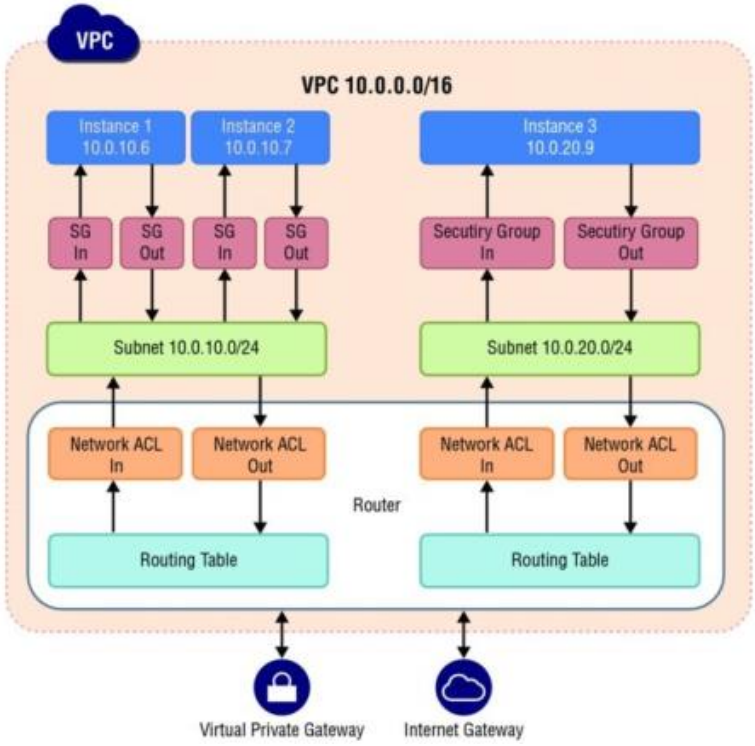
阅读公有云安全最佳实践

哪些能直接用公有云的？

- 物理安全
  - IDC
  - 存储设备退役方式

哪些能直接用公有云的？

- 网络
  - 经典网络/…. ➔大二层的共享网络
  - VPC/私有网络/…
    - 子网/虚拟交换机/…
    - 安全组
    - 网络ACL
    - VPN
    - 负载均衡(对https的支持)
    - 流日志
    - ……



哪些能直接用公有云的？

- 虚机/系统安全
  - 客户机操作系统由客户完全控制
  - 访问方式
    - 密码 vs 证书
    - 直接对外暴露 vs VPN/堡垒机

哪些能直接用公有云的？

- 数据安全
  - 对象存储/块存储/...
  - 存储安全
    - 数据完整性
    - 明文 vs 加密
  - 传输安全
    - 明文 vs SSL
  - 密钥管理
  - 证书管理

哪些能直接用公有云的？

- 管理
  - IAM/访问控制/....
    - 解决资源和权限之间的问题
    - 云平台最高权限帐号尽量少用
    - MFA
  - 审计记录
  - 监控告警

- 安全生态
  - 有无第三方安全厂商？

还需要做什么？

- 网络
  - 入侵检测/入侵防护➔IPS/NGFW
  - VPN
  - DDoS攻击
    - 硬抗
    - DNS引流➔云清洗
- 虚机/主机安全
  - 主机漏洞管理
  - 补丁管理
  - 主机IDS
  - 防病毒/恶意文件/勒索软件

还需要做什么？

- 数据安全
  - 数据库审计/管控
  - 数据加密
  - 数据备份
- 应用安全
  - WAF/云WAF
- 安全运维
  - 堡垒机

绿盟云 cloud.nsfocus.com

NSFOCUS Cloud
- SaaS安全服务
- 中国区
- 亚太区
- 北美区

公有云/行业云 安全
- AWS / Azure / Aliyun
- 腾讯云 / 青云 / 华为云 / 京东云 ...
- 深证通

安全增值能力对外提供
- SaaS模式
- 本地化模式

网站防护三步走

评估

面向互联网区域
网站安全评估服务

面向内网
极光自助扫描

紧急漏洞第一时间检测，快速评判受灾情况
紧急漏洞在线检测

满足网站公安备案要求
网站安全评估服务(公安备案版)

监测

7×24小时网站托管
网站安全监测服务

防护

适用于公有云环境
网站安全防护服务(vWAF)

面向中小客户
网站安全防护服务(主机版)

公有云安全三件套

面向网站防护
网站安全防护(vWAF)

面向安全运维
堡垒机云服务(vSASH)

面向VPN和7层防护
下一代防火墙云服务(vNF)

- 源于绿盟硬件设备
- 部署交付更简单
- 全面适配主要公有云


UCan下午茶
谢谢
有所悟
NSFOCUS
UCLOUD