QINGCLOUD青云

青云QingCloud数据与网络安全实践

黄文龙 | 青云QingCloud

青云QingCloud在做什么？

云服务
租用

云平台
建设

云架构
咨询

VM/CM | SDN&NFV | SDS | Security | Orchestration | App Center

QINGCLOUD青云

安全是云计算的重要基础

- 企业将IT系统迁移到云平台上的安全考虑
- 公有云的安全防范
- 经验与哲学

QINGCLOUD青云

青云QingCloud的多维安全架构

QINGCLOUD青云

青云QingCloud的多维安全架构

QINGCLOUD青云

网络层安全-SDN构建的虚拟网络

- 用户层面与物理层面
  - 用户层，实现传统 IT 网络环境中的组网功能
  - 物理层，将控制和转发进行分离，将控制部分提炼到软件中实现，硬件路由设备退化为二层连通设备
- 基础网络 / 私有网络
  - 基础网络是用户加入的公共网络，二层连通
  - 私有网络与其它租户完全二层隔离，足够安全，且符合传统 IT 网络构建习惯
- 二层设备 – 交换机
  - 100% 二层隔离，更高的安全性
- 三层设备 – 路由器
  - 端口转发，VPN，GRE 隧道、内网DNS

青云QingCloud的多维安全架构

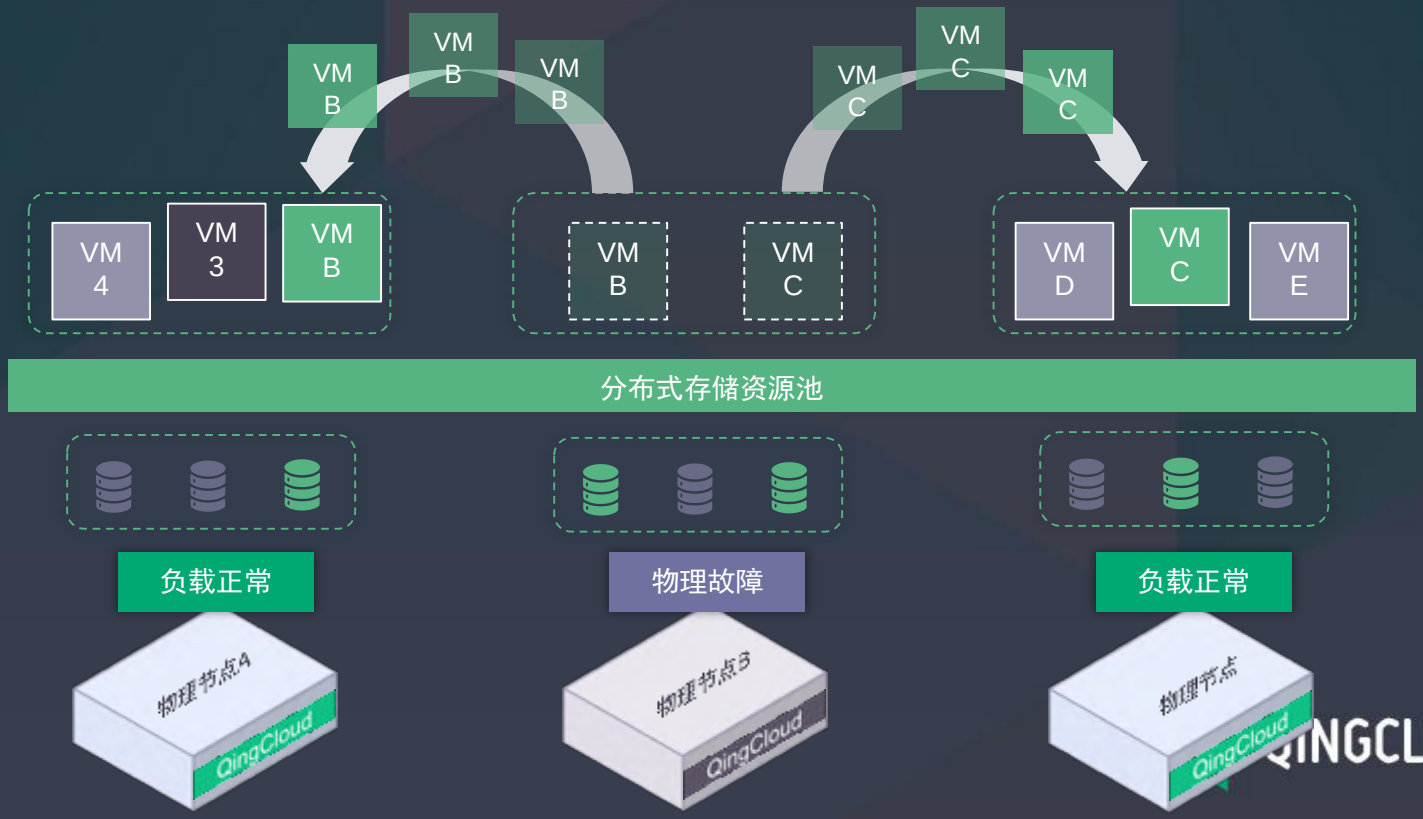
QINGCLOUD青云

云平台底层保障机制

- 实时副本与灾难恢复

实时副本在本地提供数据的可靠性保障，异地异步副本提供灾备级别保护

至少有一份不在同一个物理节点的磁盘上

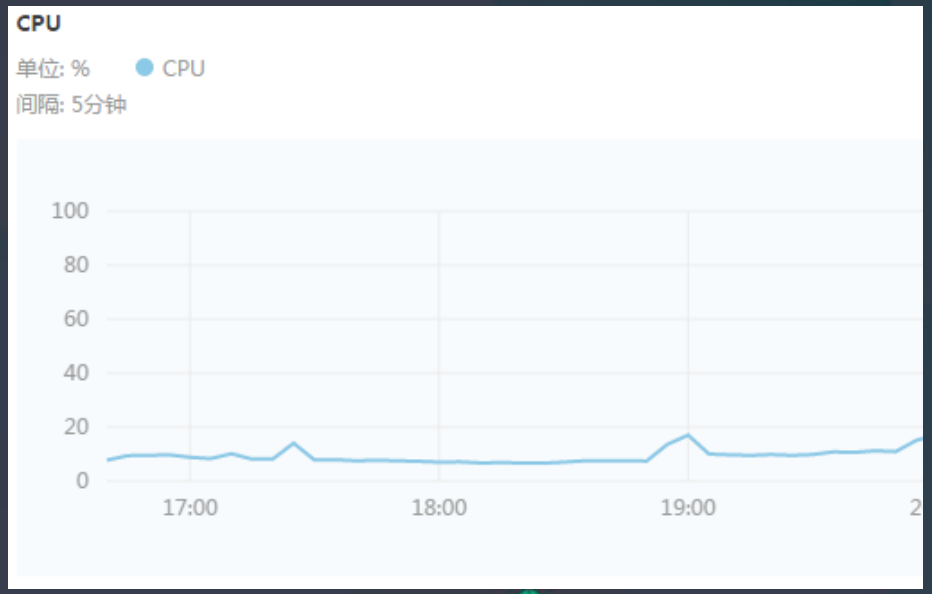


青云QingCloud的多维安全架构

QINGCLOUD青云

Hyper节点的资源监控

- 对Hyper节点进行实时监控以发现流量和性能异常
  - CPU 利用率 / 内存利用率 / 磁盘使用量 / 网络流量



QINGCLOUD青云

系统和数据的备份与恢复

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

QINGCLOUD青云

青云QingCloud的多维安全架构

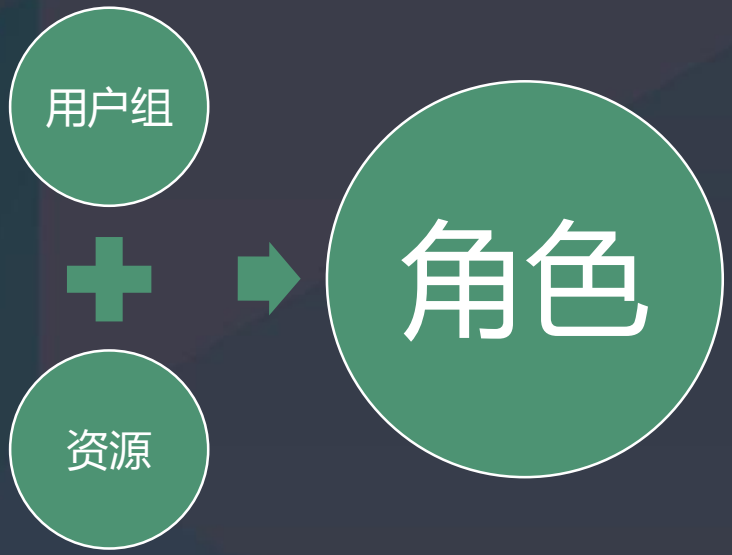
QINGCLOUD青云

云平台的认证和授权

- 统一认证 – 支持Microsoft Active Directory和LDAP
  - 只读帐号和子账户
- 云平台二次登录验证和失败告警
- 虚拟服务器登录安全 – SSH密钥绑定
  - 自由进行密钥绑定，并定期更换新密钥

QINGCLOUD青云

云平台上的账号角色与权限分配



	云资源使用者	资源权限
主账号	项目负责人	全部资源权限
子账户A	应用运维	部分云资源读写
子账户B	开发	部分云资源读写
子账户C	财务	账号充值
子账户D	审计	部分云资源读写

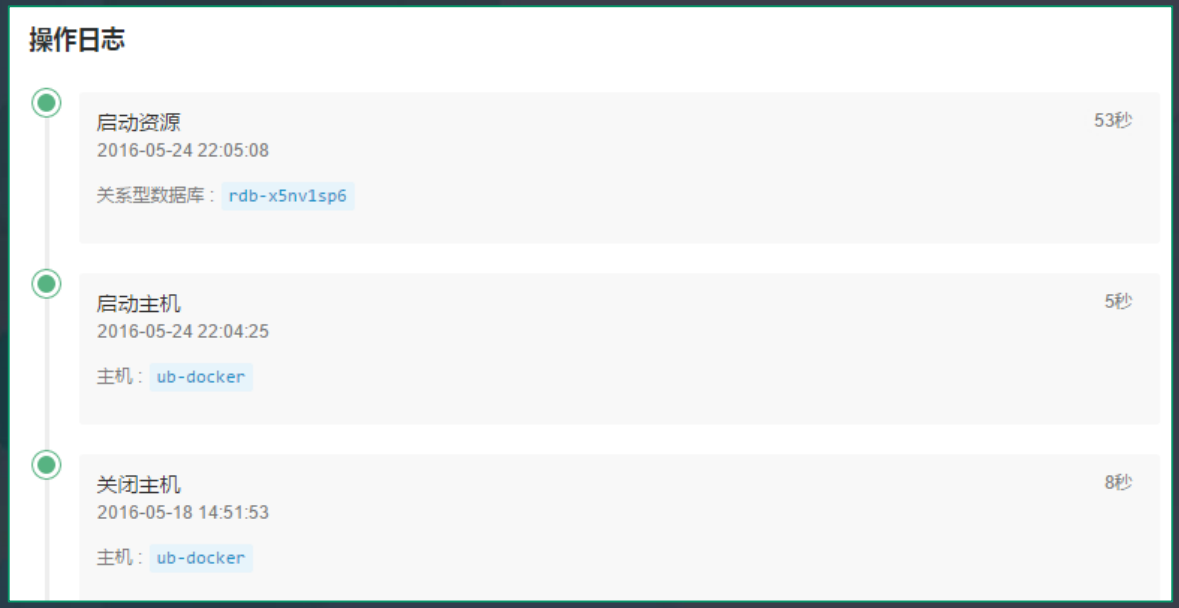
	云平台管理者	资源权限
admin	超级管理员	全部资源权限
管理员A	审计	日志管理
管理员B	后台系统运维	工单管理
管理员C	IDC管控	管理硬件资源
管理员D	审批者	审批配额申请等
管理员E	云资源管控	云资源管理，如：主机、硬盘、网络、等

资源协作的角色授权

- 配置更细粒度的权限控制
- 将资源授权给其他用户
- 实现管理和协作

QINGCLOUD青云

云平台访问日志和资源操作日志



登录时间	登录IP	登录平台	登录设备
2016-11-15 21:02:43	183.193.175.102	QingCloud 控制台	无
2016-11-13 16:19:19	183.193.175.102	QingCloud 控制台	无
2016-11-11 11:35:36	117.136.8.68	QingCloud iOS Console2.4.1	iPhone 6
2016-11-11 10:23:20	117.136.8.68	QingCloud 控制台	无
2016-11-10 23:05:26	183.193.141.104	QingCloud 控制台	无
2016-11-10 10:10:50	116.228.58.93	QingCloud 控制台	无

QINGCLOUD青云

公有云上的安全保护

面向互联网的安全保护

QINGCLOUD青云

构建云安全生态

专业的人做专业的事

QINGCLOUD APPCENTER
青云应用中心

NSFOCUS

唐朝安全巡航 TangScan.com

QINGCLOUD青云

QingCloud应用中心的安全服务

已安装

安全宝

安全宝是国内第一款基于云服务的网络安全品牌，全身心致力于为网站提供专业、细致的云安全

免费

已安装

青松抗D

青松抗D提供DDoS防御解决方案及服务，简单快捷，有效缓解DDoS攻击带来的业务和品牌信誉

¥ 10 每小时 起

已安装

牛盾云安全

安全、加速、稳定、智能DNS。

免费

已安装

三未信安云密码服务

提供云环境中对数据加密、身份认证及数字签名的需求

免费

已安装

百度云观测

云观测是百度云安全部旗下的云服务产品。只需三步添加网站，即可一站式获得内容、漏洞、可

免费

已安装

网蛙神探

网蛙神探，Android,IOS应用漏洞扫描服务

免费

TangScan

Tangscan为企业提供安全漏洞监测与风险及资产管理服务。

免费

已安装

服务器安全狗 Linux版

国内首款免费的Linux服务器安全软件，抗攻击、防入侵，全方位守护您的服务器安全！

免费

已安装

服务器安全狗 Windows版

安全防黑首选，市场占有率第一

免费

QINGCLOUD青云

云计算中的应用安全

- XSS 跨站脚本攻击
- SQL 注入攻击
- CSRF 跨站请求伪造
- 恶意爬虫
- 文件上传漏洞
  - 锐御RayWAF

相较于传统的防火墙和入侵防御系统，锐御更专注于WEB 应用自身的漏洞。锐御不仅用于保护面向互联网的WEB 应用，还可以被部署在内部WEB 应用服务器之前，对内部的业务访问进行访问控制和业务审计，并防范来自内部的威胁。

云计算中的拒绝服务攻击

- Challenge Collapsar 攻击 / SYN Flood / 慢速攻击
- 攻击者向某一 IP 发送大规模的数据包流量
  - 目的是占满被攻击者的总入口带宽，使正常流量无法进出
  - 通常由上层网络提供者发现和处理，云计算的终端用户无法直接干预
- 青云与数据中心合作应对大规模流量攻击
  - 动态修改被攻击对象的链路到隔离链路，避免影响全局
  - 广播 IP 路由到上联机房交换机，将流量牵引到黑洞清洗设备
  - DDOS高级防护服务

QINGCLOUD青云

青云QingCloud获得的一系列认证

- ICP经营许可证
- IDC/ISP资质证书
- 等保三级证书
- ISO9001质量管理体系证书
- ISO27001信息安全管理体系证书（办理中）
- 可信云认证证书（云主机认证）
- CMMI3级软件成熟度模型评估证书
- ITSS服务能力评测证书（办理中）

QINGCLOUD青云

经验与哲学

- 推出的每一项功能都必须是出众的，和别人做的一样就没有任何机会
- 人是最容易出错的，所有能够被自动化的事情，都需要被自动化
- 对代码质量的极致追求，不断地 Refactoring
- 一切出错都应该控制在局部范围内，避免影响全局
- 系统的任何部分都应该是可水平扩展的
- 逻辑可以是复杂的，架构一定是简洁的
- 构建完整的云安全生态体系


QINGCLOUD青云

关注我们

QingCloud-IaaS

青云QingCloud

www.qingcloud.com

QINGCLOUD青云

Thank you.

huangwenlong@yunify.com