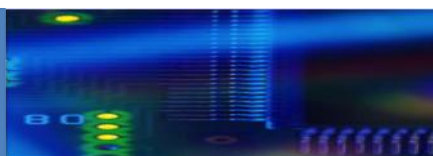




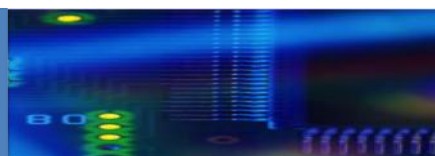
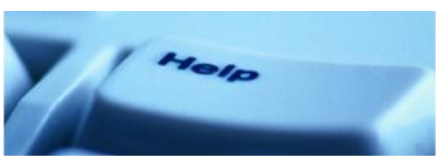
校园云服务和安全管理

大连理工大学网络与信息化中心
于广辉



议程

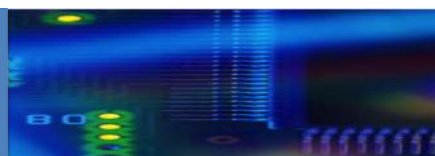
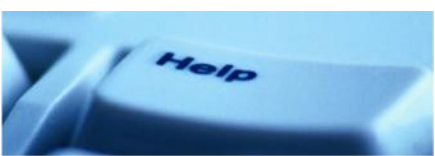
- 校园云服务
- 校园云服务实践
- 校园云服务安全管理
- 软件定义下的校园云服务



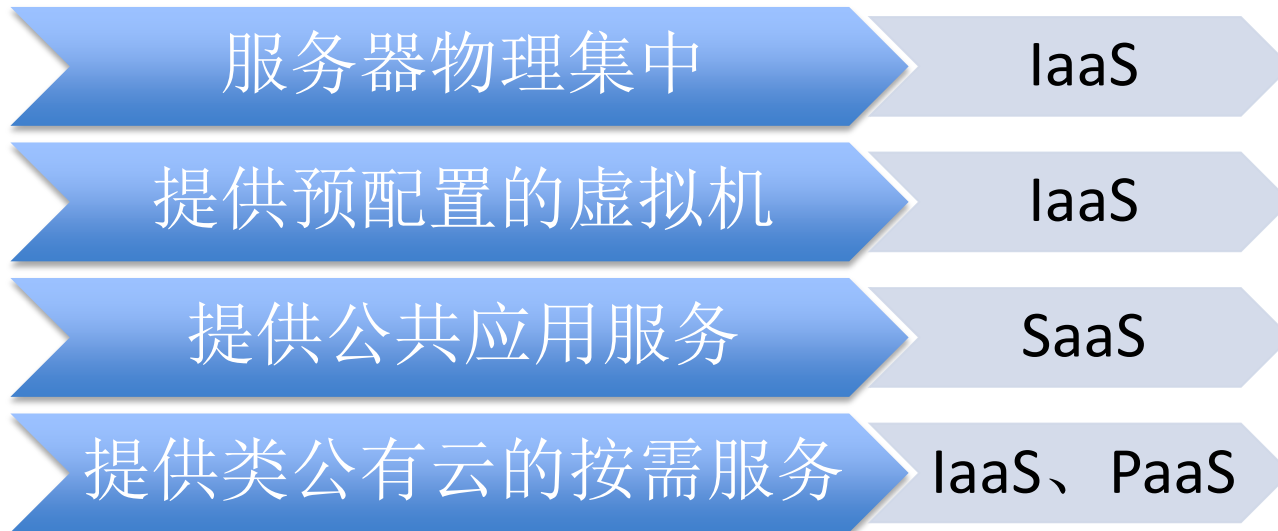
校园云服务

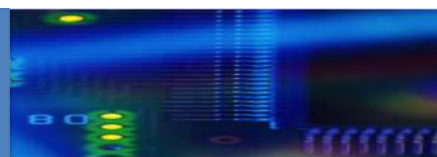
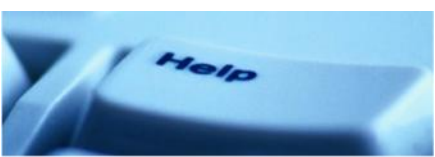
	校园云服务	企业私有云	公有云
服务对象	信息化核心应用	企业核心应用	公众用户
	校内师生		
管理权限	应用级	深入到应用内部	基础设施
	基础设施		
服务规模	上千虚拟机量级	上百虚拟机量级	上百万虚拟机量级
计费模式	按量计费	纳入企业成本	按量计费

建立在校园内部的公有云和私有云的混合体，在管理和架构上同时具有私有云和公有云的特点。



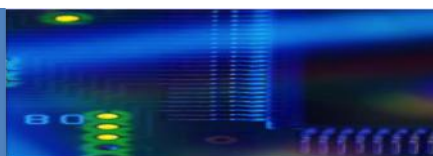
管理模式的变化





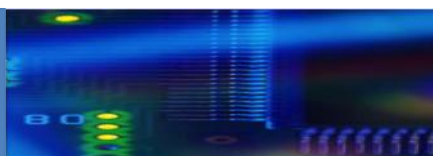
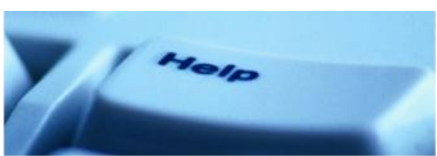
公共应用服务

- 不能纳入信息化基础或核心应用的，具有共性的
在线服务
 - Web视频会议系统
 - 网站群系统
 - 问卷调查系统
 - 会议网
 - 高性能计算服务
 - 正版软件服务



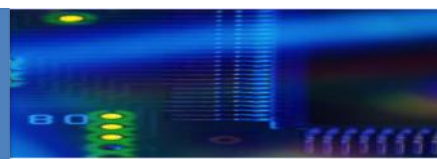
类公有云的按需服务

- 用户个人申请的云主机及相关服务
- 区别完整的租户概念
- 根据模版生成
- 按量计费



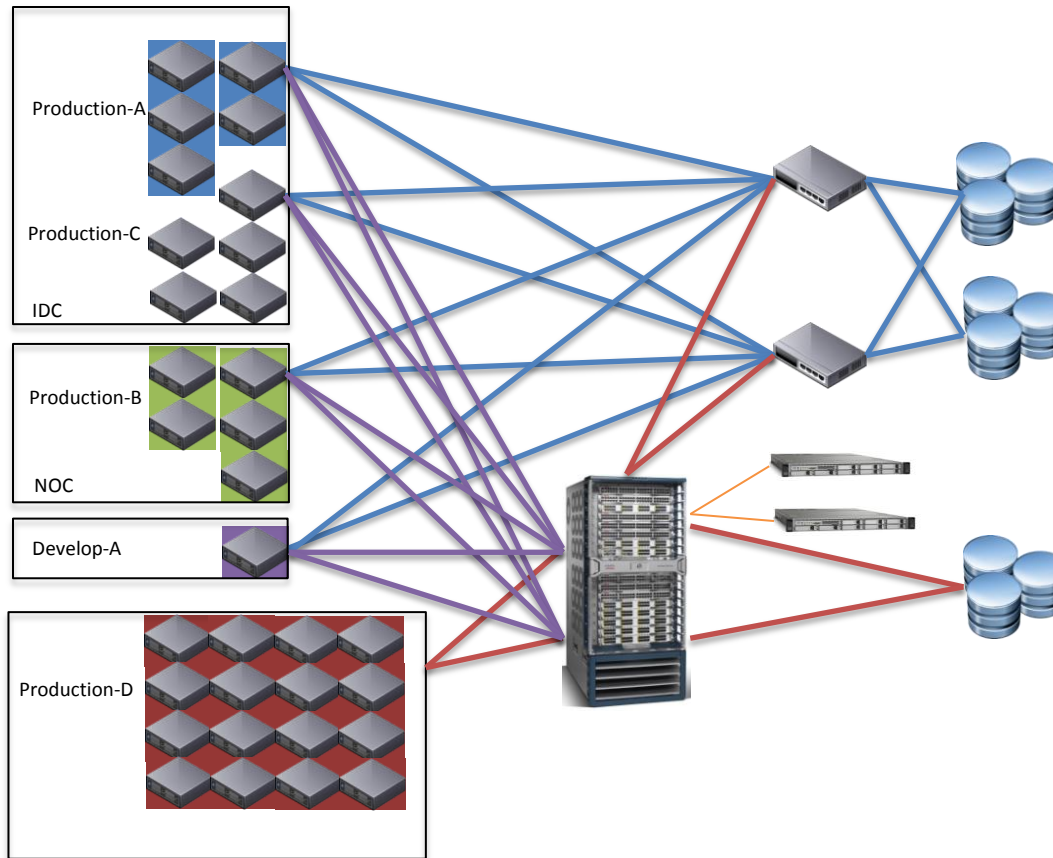
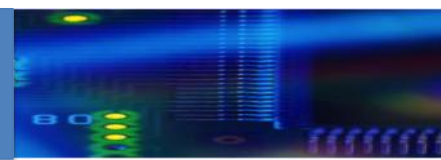
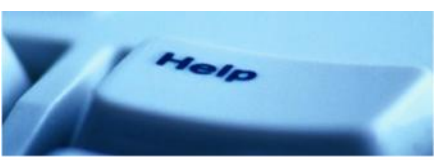
议程

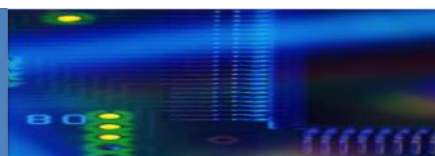
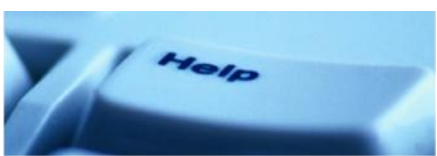
- 校园云服务
- **校园云服务实践**
- 校园云服务安全管理
- 软件定义下的校园云服务



校园云数据中心概况

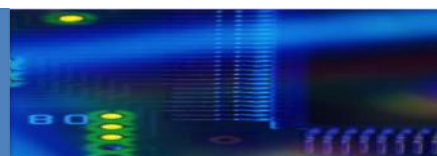
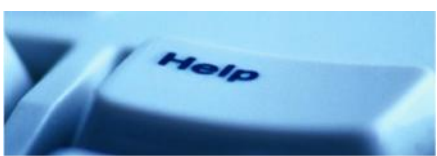
- 2003年开始建设数据中心
- 2007年实施服务器虚拟化工作，经过两次扩容
 - 32台物理服务器
 - 118颗CPU，9.4TB内存，200TB存储
 - 500余台虚拟服务器
- 包括信息化核心应用、一卡通等全部业务





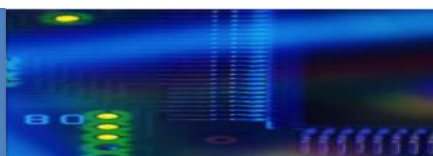
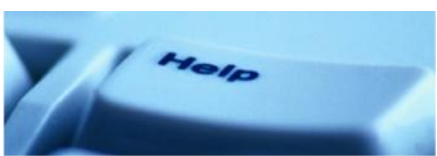
连续9年无故障运行

名称	状况	状态	正常运... 1 ▲	群集	CPU 百分比(%)	内存百分比(%)
vm16.dlut.edu.cn	已连接	✔ 正常	16 天	Production-D	0	3
vm07.dlut.edu.cn	已连接	✔ 正常	16 天	Develop-A	11	45
vm06.dlut.edu.cn	已连接	✔ 正常	16 天	Develop-A	3	26
vm11.dlut.edu.cn	已连接	✔ 正常	16 天	Production-B	4	26
vm10.dlut.edu.cn	已连接	✔ 正常	16 天	Production-B	4	14
vm09.dlut.edu.cn	已连接	✔ 正常	16 天	Production-B	11	23
vm19.dlut.edu.cn	已连接	✔ 正常	20 天	Production-C	0	1
vm13.dlut.edu.cn	已连接	✔ 正常	21 天	Production-D	1	11
vm04.dlut.edu.cn	已连接	✔ 正常	44 天	Production-B	11	38
vm05.dlut.edu.cn	已连接	✔ 正常	44 天	Production-B	9	30
vm15.dlut.edu.cn	已连接	✔ 正常	44 天	Production-D	2	12
vm14.dlut.edu.cn	已连接	✔ 正常	44 天	Production-D	3	13
vm12.dlut.edu.cn	已连接	⚠ 警告	45 天	Production-D	3	12
vm32.dlut.edu.cn	已连接	✔ 正常	46 天	Production-E	0	3
vm31.dlut.edu.cn	已连接	✔ 正常	48 天	Production-E	2	33
vm30.dlut.edu.cn	已连接	✔ 正常	48 天	Production-E	2	35
vm18.dlut.edu.cn	已连接	✔ 正常	50 天	Production-C	9	28
vm23.dlut.edu.cn	已连接	✔ 正常	51 天	Production-E	6	23
vm29.dlut.edu.cn	已连接	✔ 正常	51 天	Production-E	10	27
vm28.dlut.edu.cn	已连接	✔ 正常	51 天	Production-E	7	31
vm27.dlut.edu.cn	已连接	✔ 正常	51 天	Production-E	3	24
vm26.dlut.edu.cn	已连接	✔ 正常	51 天	Production-E	10	20



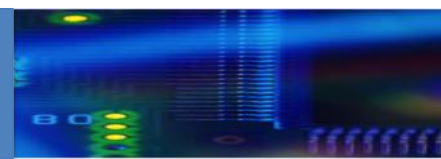
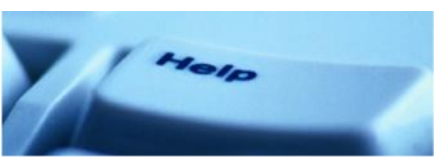
我们看到的校园云数据中心优势

- 建设成本
 - 初始投入高，生命周期长
 - 硬件资源可以重复使用，承载不同的应用系统。
- 管理成本下降
 - 500余台虚拟机，信息部2个人管理
- 升级、迁移成本下降
- 为信息化建设提供有效支撑
 - 快速部署
 - 可控运维
 - 统一安全防护
 - 为学校信息化统一管理提供基础支撑。
- 能耗下降
- 虚拟化平台运行稳定，9年无宕机
 - 业务系统9年连续运行
 - 应用系统整体停机只有1小时（早期单存储时，升级存储硬盘固件）



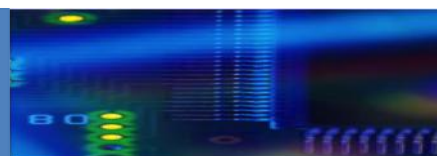
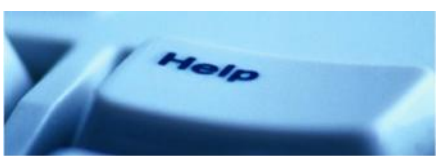
议程

- 校园云服务
- 校园云服务实践
- **校园云服务安全管理**
- 软件定义下的校园云服务



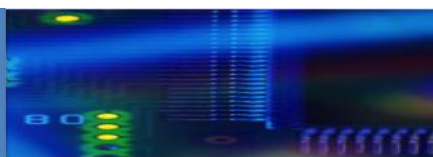
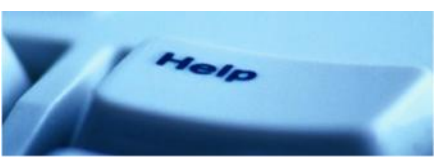
信息主管部门的角色和定位

- 上级监管的压力
- 有限的权利、经费、人力，无限的责任
- 保镖？消防员？警察？法官？
- 谁主管谁负责、谁运维谁负责、谁使用谁负责？



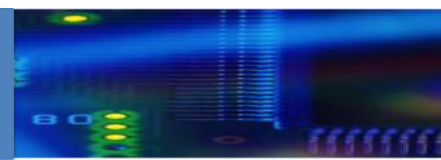
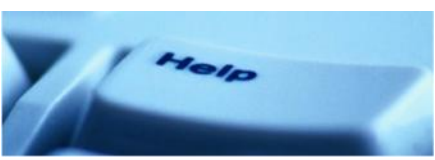
习总书记如何看待网络安全

- 网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。
 - 2014年2月27日习近平主持在中央网络安全和信息化领导小组第一次会议的重要讲话
- 网络安全是整体的而不是割裂的；网络安全是动态的而不是静态的；网络安全是开放的而不是封闭的；网络安全是相对的而不是绝对的；网络安全是共同的而不是孤立的。
 - 2016年4月19日习近平总书记网络安全和信息化工作座谈会上的讲话



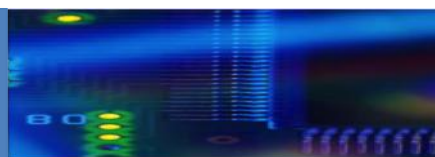
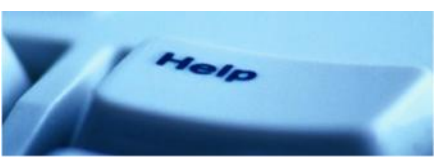
甲方安全

- 懂业务
- 三分技术七分管理
- 面宽，深入度不够
- 乙方提供的解决方案往往是网络安全和应用安全的基础性安全措施
- 安全风险管理的



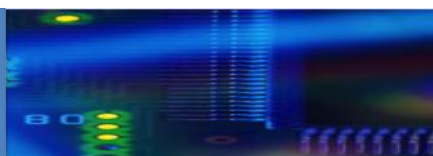
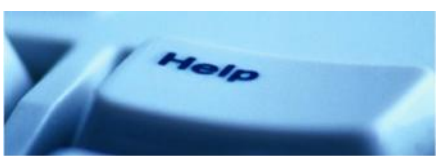
甲方安全

- 技术解决不了的问题管理解决
- 管理解决不了的问题技术解决



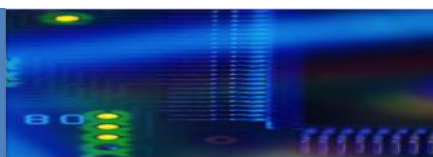
管理制度

- 成立“网络安全与信息化建设管理委员会”
- 《信息化建设管理办法》
- 《信息化数据管理办法》
- 《学校办公室关于加强校内信息安全管理工作的通知》
- 校内域名管理办法、学校二级网站管理办法
- 内部的服务器管理员操作手册（Linux版和Windows版）、堡垒机操作手册等
- 动环运维的管理制度



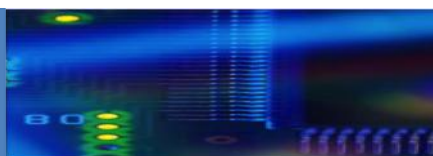
逐步建立内外部运维审计制度

- 制度+技术
- 外部服务商必须通过外部运维堡垒机
 - 口令+二次认证
- 内部关键业务逐步强制通过内部运维堡垒机
- 关键配置审查
- 关键操作审查
- 敏感数据访问审批



建立自动化备份机制

- 虚拟化平台级自动化备份
- 关键业务连续备份
- 磁带库二级应用备份
- 重点应用使用磁带库日备、周备、月备



虚拟化平台级自动化备份

The screenshot displays a backup management interface with a table of replication jobs and a summary panel.

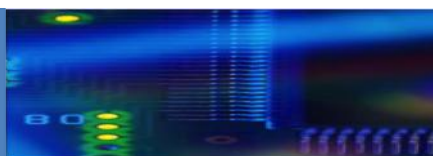
名称	状态	类型	上次开始时间	持续时间	下次运行时间	成功计数	失败计数
MainGroup1	启用	映像	2016/03/30 09:30	0h:23m:9s	2016/04/06 10:00	26	0
MainGroup2	启用	映像	2016/03/31 07:30	2h:48m:19s	2016/04/07 07:30	17	0

Summary Panel (Replication Jobs):

- Period: Last 24 hours
- Failed: 0
- Pending: 0
- Running: 0
- Succeeded with Exception: 0
- Succeeded: 0

Status Bar: ✓ Sch/Disp: Running/Running | ✓ No Unacknowledged Events | ✓ Server: Full Access





关键业务连续备份

出站复制

入站复制

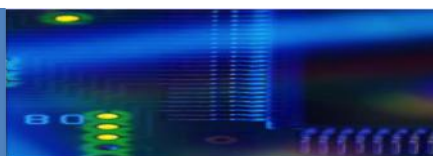
报告

虚拟机	状态	目标	同步点	RPO
ykt_centos_...	良好	jasmine.dlut...	16/4/22 下午1:57	15分钟
carnation	良好	jasmine.dlut...	16/4/22 下午2:03	15分钟

2个项目

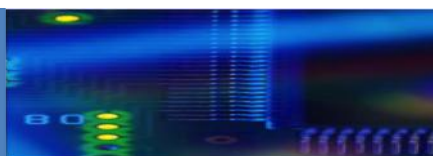
复制详细信息 时间点

虚拟机:	ykt_ce...	状态:	良好	RPO:	15分钟
目标站点:	jasmin...	上次同步持续时间:	2秒	静默:	无
VR 服务器:	VRA	上次实例同步点:	16/4/22 下午1:57		
		上次同步大小:	9.86 MB		



部署云管理平台

- 将核心平台和最终用户隔离
- 将Vmware或未来其他虚拟化平台作为资源池统一管理
- 实现模版自动部署
- 实现按使用量计费



计费模板 > 创建计费模板

服务名 (*) 服务A

操作系统类型 (*) Windows

计费模板名称 (必) 操作系统 (*) Microsoft Windows 7

资源模板 (必) 默认模板

我的虚拟机

每页显示 10 条记录

虚拟机名称	服务名称	状态	到期日期	状态	
smpvm01	服务A	使用中	2016-04-23	开机	
test-555	服务A	使用中	2098-02-04	关机	

10

内存范围结束数值(单位: GB)

数据盘 (*) 40

数据盘范围起始数值(单位: GB)

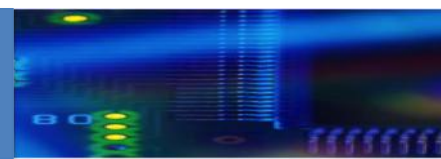
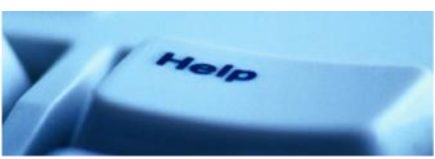
400

数据盘范围结束数值(单位: GB)

保存 返回

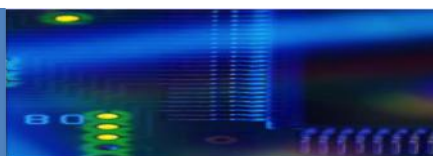
字数:

虚拟机服务名称

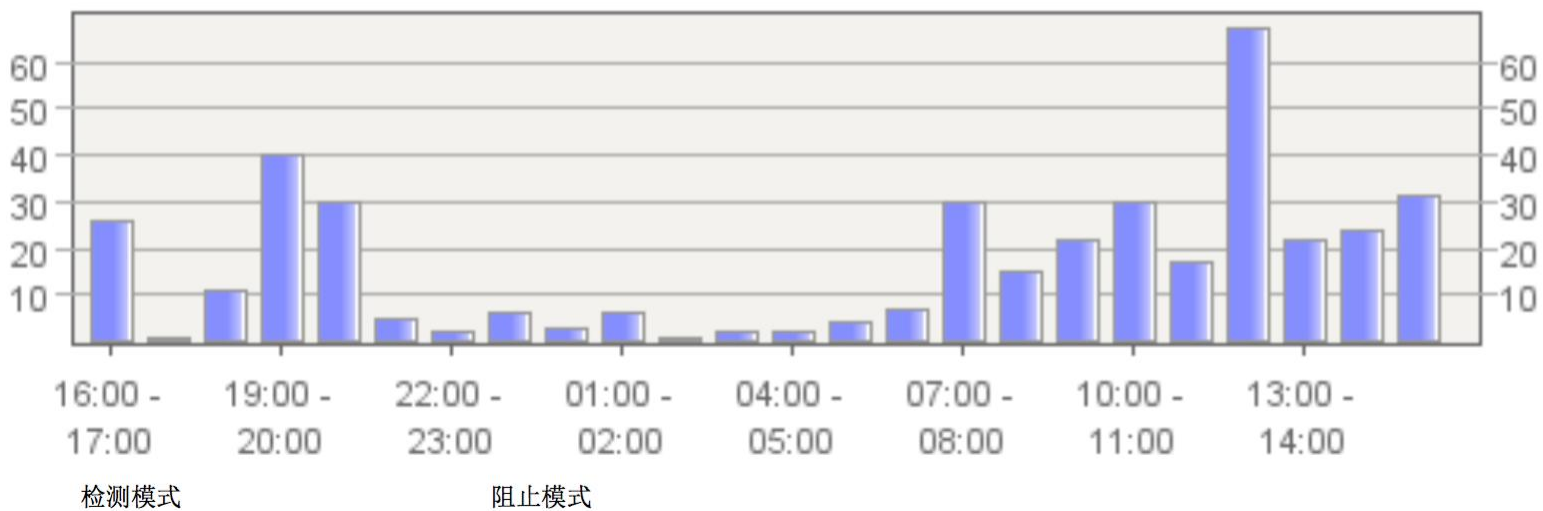


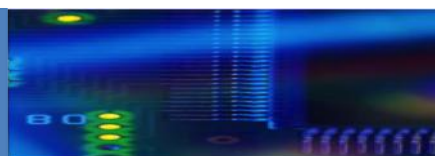
网络安全策略

- 校园网边界启用状态防火墙，默认只允许校内向校外单向访问
- 数据中心对校外开放特定端口
- 个别非数据中心服务及非标准端口开放服务需要经过审批
- 云平台进行统一的安全防护
 - WAF（硬件）
 - 无代理防病毒（平台软件）
 - 虚拟补丁（平台软件）
 - 包过滤防火墙、IPS（平台软件）
- 正在计划实施数据中心白名单制度，深度检测，只允许已登记的应用提供服务



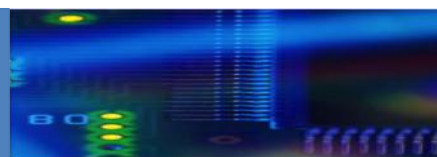
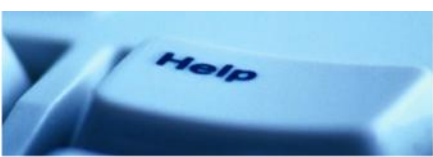
入侵防御事件历史记录





零信任的VPN服务

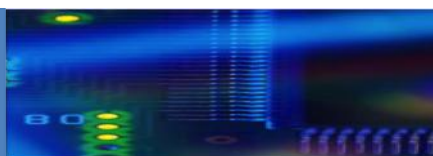
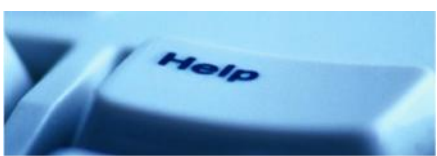
- 大并发容量
- 应用级别可管理性
- 不能成为安全系统的后门
- 可审计



(rule eq 'VPN Default Policy')

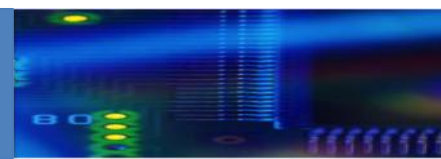
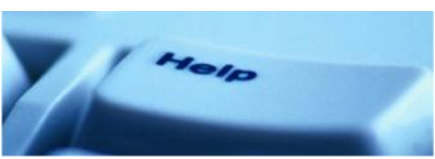


	Match Time	Update Time	Object Name	Source address	Source User	Severity	Summary
	2016/07/06 13:32:34	2016/07/07 10:12:31	Beacon Detection	10.100.5.34	2010099194	medium	Host visited known malware URL (100 times).
	2016/07/07 09:02:03	2016/07/07 09:02:03	Beacon Detection	10.100.6.13	2005011026	medium	Host visited known malware URL (15 times).
	2016/07/07 08:25:38	2016/07/07 08:25:38	Beacon Detection	10.100.7.171	2001011050	medium	Host visited known malware URL (19 times).
	2016/07/06 21:56:53	2016/07/06 21:56:53	Beacon Detection	10.100.3.218	2006011129	medium	Host visited known malware URL (75 times).
	2016/07/06 21:11:03	2016/07/06 21:11:03	Beacon Detection	10.100.1.59	2008011158	medium	Host visited known malware URL (33 times).
	2016/07/06 19:33:36	2016/07/06 19:33:36	Beacon Detection	10.100.2.211	2013011209	medium	Host visited known malware URL (68 times).
	2016/07/06 18:54:01	2016/07/06 18:54:01	Beacon Detection	10.100.7.229	2014011231	medium	Host visited known malware URL (19 times).
	2016/07/06 18:34:53	2016/07/06 18:34:53	Beacon Detection	10.100.5.56	1970011001	medium	Host visited known malware URL (16 times).
	2016/07/06 14:30:27	2016/07/06 17:14:07	Beacon Detection	10.100.4.25	1993011042	medium	Host visited known malware URL (100 times).
	2016/07/06 16:33:09	2016/07/06 16:33:09	Beacon Detection	10.100.4.177	2008011057	medium	Host visited known malware URL (46 times).
	2016/07/06 16:27:41	2016/07/06 16:27:41	Beacon Detection	10.100.2.9	2005011070	medium	Host visited known malware URL (13 times).
	2016/07/06 14:30:41	2016/07/06 14:30:41	Beacon Detection	10.100.7.209	2013011231	medium	Host visited known malware URL (22 times).
	2016/07/06 11:08:16	2016/07/06 11:08:16	Beacon Detection	10.100.0.224	1996011053	medium	Host visited known malware URL (11 times).
	2016/07/06 11:08:15	2016/07/06 11:08:15	Beacon Detection	10.100.0.179	2004011004	medium	Host visited known malware URL (12 times).
	2016/07/06 10:40:25	2016/07/06 10:40:25	Beacon Detection	10.100.2.236	2014011025	medium	Host visited known malware URL (23 times).
	2016/07/06 09:29:37	2016/07/06 09:29:37	Beacon Detection	10.100.0.113	2010011013	medium	Host visited known malware URL (78 times).
	2016/07/06 08:37:06	2016/07/06 08:37:06	Beacon Detection	10.100.1.50	1995011002	medium	Host visited known malware URL (48 times).
	2016/07/05 23:17:25	2016/07/05 23:17:25	Beacon Detection	10.100.2.236	2014011025	medium	Host visited known malware URL (18 times).
	2016/07/05 22:27:50	2016/07/05 22:27:50	Beacon Detection	10.100.7.221	2013011247	medium	Host visited known malware URL (13 times).
	2016/07/05 22:20:50	2016/07/05 22:20:50	Beacon Detection	10.100.1.20	2015011159	medium	Host visited known malware URL (14 times).



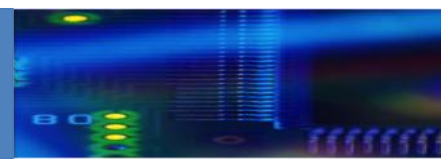
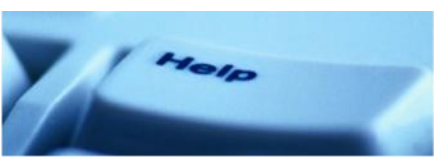
议程

- 校园云服务
- 校园云服务实践
- 校园云服务安全管理
- 软件定义下的校园云服务



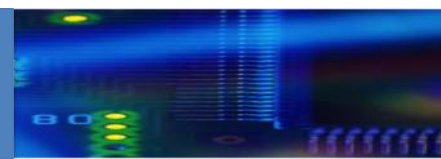
对管理视角理解的变化

- 管理复杂度由量变到质变
- 以应用为中心
- 从网络管理员角度出发到以应用管理员角度出发
- 网络（安全）管理员的责任：
 - 提供和维护通用的模版策略
- 应用（系统）管理员
 - 根据应用性质做菜单式选择



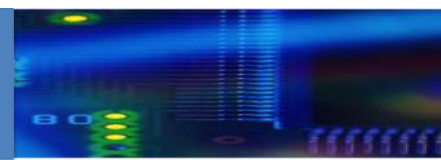
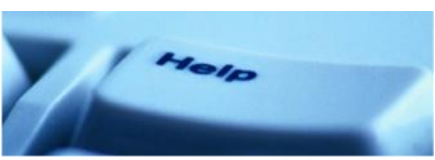
对设备性能理解的变化

- 有效的业务流量
 - 对业务流量的精细化分析和管理的
 - 有效业务流量比预期的要少的多
- 需求的变迁
 - 性能不在是关注的重点
 - 能够满足业务流量需要的设备都是好设备
 - 对业务流量的深度分析更加重要
 - 能够纳入云平台统一管理更加重要

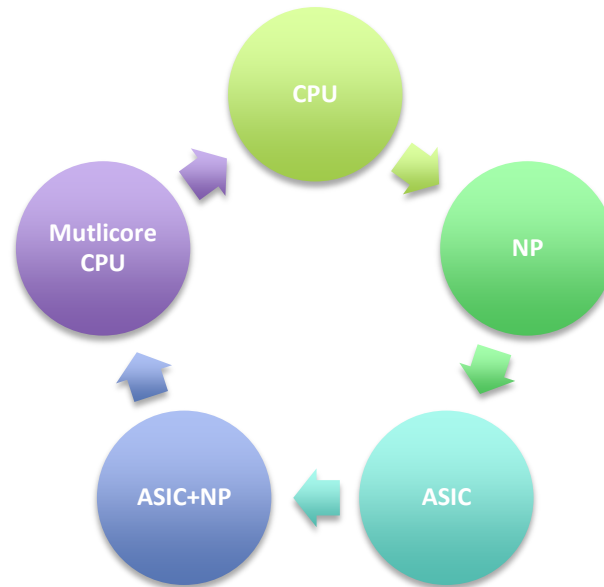


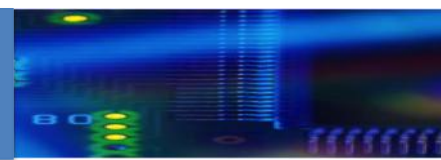
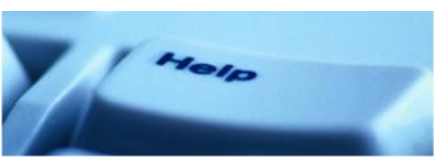
我们看到的趋势

- 在大规模的软件定义数据中心部署中，传统的物理网络、安全设备不在有优势
 - 在虚拟机之间进行东西向控制过于复杂
- 基于软件的虚拟设备将取代部分物理安全设备
 - 无代理的防病毒层
 - 控制东西向流量安全策略的分布式交换机和防火墙
 - 南北向流量设备（路由器、VPN、防火墙、IPS、WAF等）
- 基于特征的安全技术将被基于行为的安全技术替代
 - 传统的基于特征的方法已经无法满足当前安全需要
 - 沙箱？基于主机的行为？基于网络的行为？



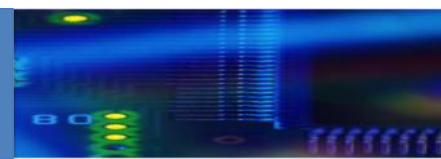
软件硬件的轮回





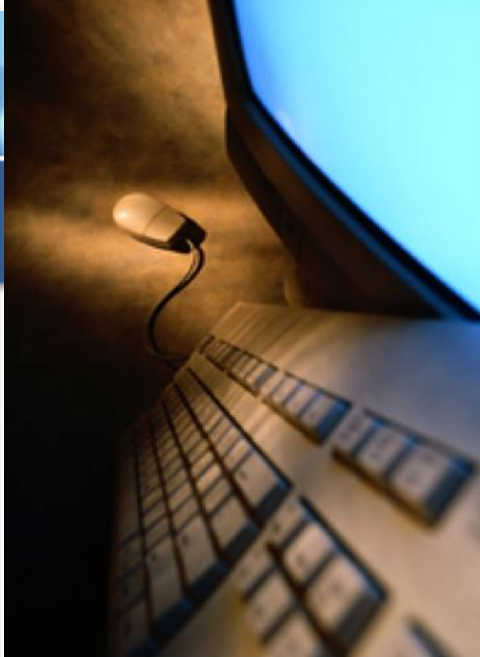
基础设施和软件定义的融合

- 能感知到虚拟机，并动态调整控制策略。
- 能同虚拟化交换机一体化管理，将虚拟设备作为基础设施的延伸。
- 3-7层业务编排同云平台相结合
 - 按需部署的虚拟机模版、虚拟设备（防火墙、负载均衡、VPN等）
- 虚拟设备通过云平台统一管理
 - 从应用管理员视角出发，模版式部署策略



我们现在关心的问题

- 安全
 - 信息化是双刃剑，集中了业务和数据的同时也集中了风险和责任
 - 法律和伦理的地带，大数据与隐私保护
- 应用
 - 原有应用平滑过度
 - 新增应用是真正为云计算设计（不是简单的搬家）
- 完整的云战略
 - 外部公有云使用的原则
 - 潜在的风险，风险管理和灾难恢复



谢谢