国家信息中心
State Information Center

政务云测评发现及安全保障建议

汇 报 人：尚庆军
时　　间：2018年12月27日

1 政务云建设管理模式

2 政务云特点及安全挑战

3 政务云安全检测中发现的主要问题

4 政务云安全保障建议

政务云建设管理模式

一、政务云建设管理模式多样

运营模式	云服务方	云服务客户	产品和服务提供商	运维方
政府建设 政府自用 政府维护 私有云	政府	各委办局	云平台开发商和设备厂商	政府人员，云平台开发商和设备厂商（提供一定运维服务）
政府建设 政府自用 运营商维护 私有云	政府	各委办局	运营商，云平台开发商和设备厂商	运营商，云平台开发商和设备厂商（提供一定运维服务）
运营商建设 运营商维护 政府整体购买服务 私有云	运营商	政府-委办局（二级）	运营商，云平台开发商和设备厂商	运营商，云平台开发商和设备厂商（提供一定运维服务）
运营商建设 运营商维护 政府按需购买服务 公有云或混合云	运营商	政府-委办局（二级），其他企事业单位	运营商，云平台开发商和设备厂商	运营商，云平台开发商和设备厂商（提供一定运维服务）

自采、自建、自维

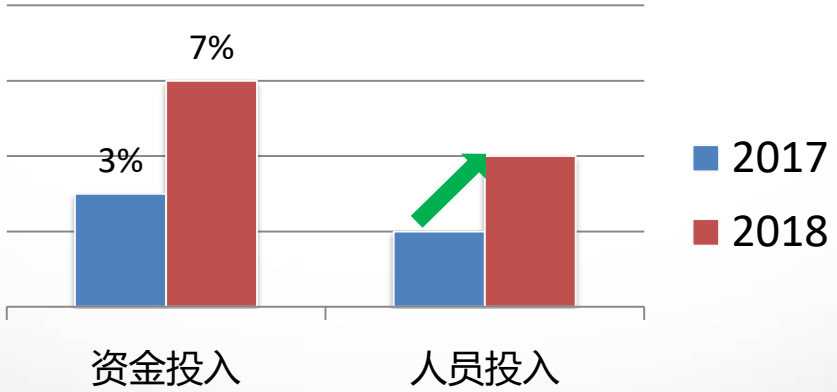
自采、自建、他维

采购服务模式

- 二、政务云正从“可用优先”向“安全与可用并重”转变

提供稳定的政务服务

提供安全可靠的政务服务



1 政务云建设管理模式

2 政务云特点及安全挑战

3 政务云安全检测中发现的主要问题

4 政务云安全保障建议

政务云系统特点

云计算的本质、特征、功能等适用于完成电子政务3项重点工作

- 最大限度地实现**资源共享**
- 最大限度地实现政务**业务协同**
- 以及最大限度地实现**互联互通**

物理资源整合

- 建设云计算平台，提供基础设施服务
- 建设电子政务灾备中心
- 整合数据中心

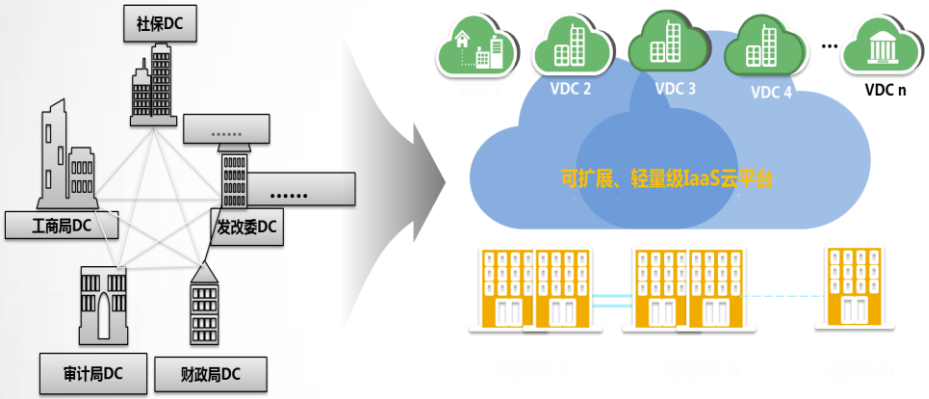
数据共享和协同办公

- 政务部门业务迁移
- 政务信息资源共享交换应用服务示范

数据和应用整合

- 跨部门应用整合
- 基于构建统一、融合的基础数据
- 跨部门、跨行业、跨区域的政务信息资源共享

政务云的安全挑战



- **业务涉及多朵云：政务专有云、政务公有云**
- **多地中心：主生产中心、灾备中心**
- **网络场景复杂：物理专网、逻辑专网、政务外网、政务互联网、涉密内网、机房延伸、跨云数据交换**
- **局委办业务众多：公积金、财政、工商、税务、国资、安监局、发改委等50+个单位，120+套业务系统**

政务云面临的主要安全挑战

1.云平台安全防护责任重

- 云平台承载局委办核心业务，且大部分定义为关键信息基础设施，安全可控程度要求高；
- 关键业务多，数据交换多，如何保障数据安全。

2.受攻击面广，保障压力大

- 委办局业务上云安全需求多样化，但普遍安全基础薄弱，传统方案难部署难调整；
- 专业的安全管理和运维人员缺乏。

3.安全监管要求高，安全责任重

- 面临关键信息基础设施保护、等级保护、个人隐私保护、数据开放安全等多项安全监管

4.要求快速、高效的安全管理

- 海量安全事件难以及时处理，难以准确定位关键威胁和快速响应

1 政务云建设管理模式

2 政务云特点及安全挑战

3 政务云安全检测中发现的主要问题

4 政务云安全保障建议

政务云的测评要求

等级保护2.0基本要求
等级保护2.0云扩展要求

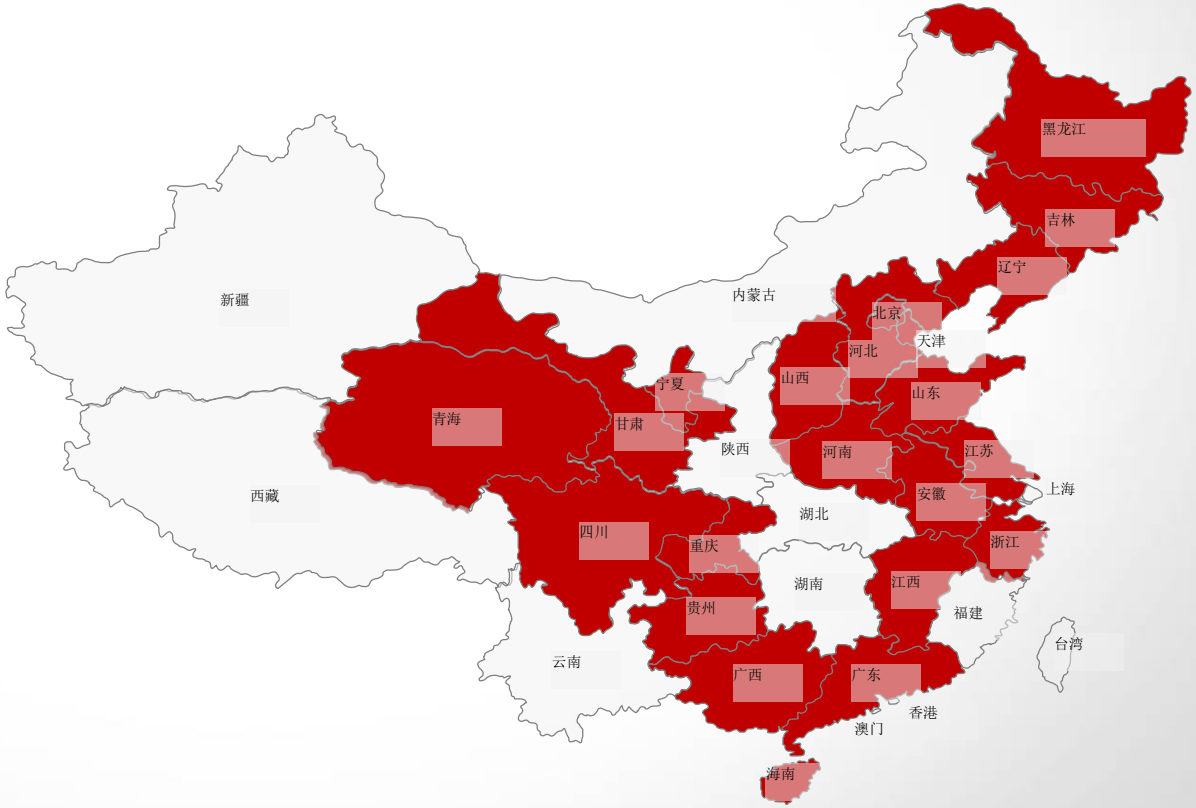
- 《信息安全技术 网络安全等级保护实施指南》
- 《信息安全技术 网络安全等级保护安全设计技术要求》
- 《信息安全技术 网络安全等级保护测评过程指南》
- 《信息安全技术 网络安全等级保护测评要求》

政务行业标准

- 《政务云安全要求》
- 《国家电子政务外网等级保护实施指南》
- 《国家电子政务外网等级保护基本要求》
- 《国家电子政务外网跨网数据安全交换技术要求与实施指南》
- 《国家电子政务外网局域网安全技术规范》
- 《国家电子政务外网电子认证管理办法》

案例范围

- 服务模式IAAS、PAAS
- 私有云、混合云
- 超过60%省已开展政务云平台及租户系统测评

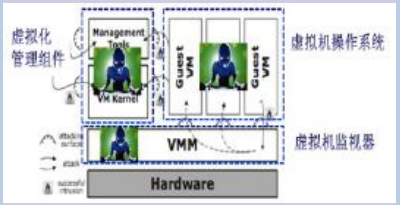


政务云平台安全问题

虚拟化问题

虚拟化技术漏洞引入的安全问题

- 租户镜像不加密存储，导致租户信息泄露
- 虚拟机监视器问题
- 虚拟机操作系统漏洞
- 宿主机防护不足



云平台问题

恶意租户攻击带来的安全问题

- 恶意租户可通过共享资源对云计算基础设施进行攻击
- 租户间攻击导致数据泄露
- 正常租户被控制后，可被当作工具发起攻击

云管平台被恶意入侵带来的安全问题

- 租户信息泄露
- 云管平台存在后门程序，致使越权操作
- 云管平台被攻陷，随意启、停、删除虚机实例

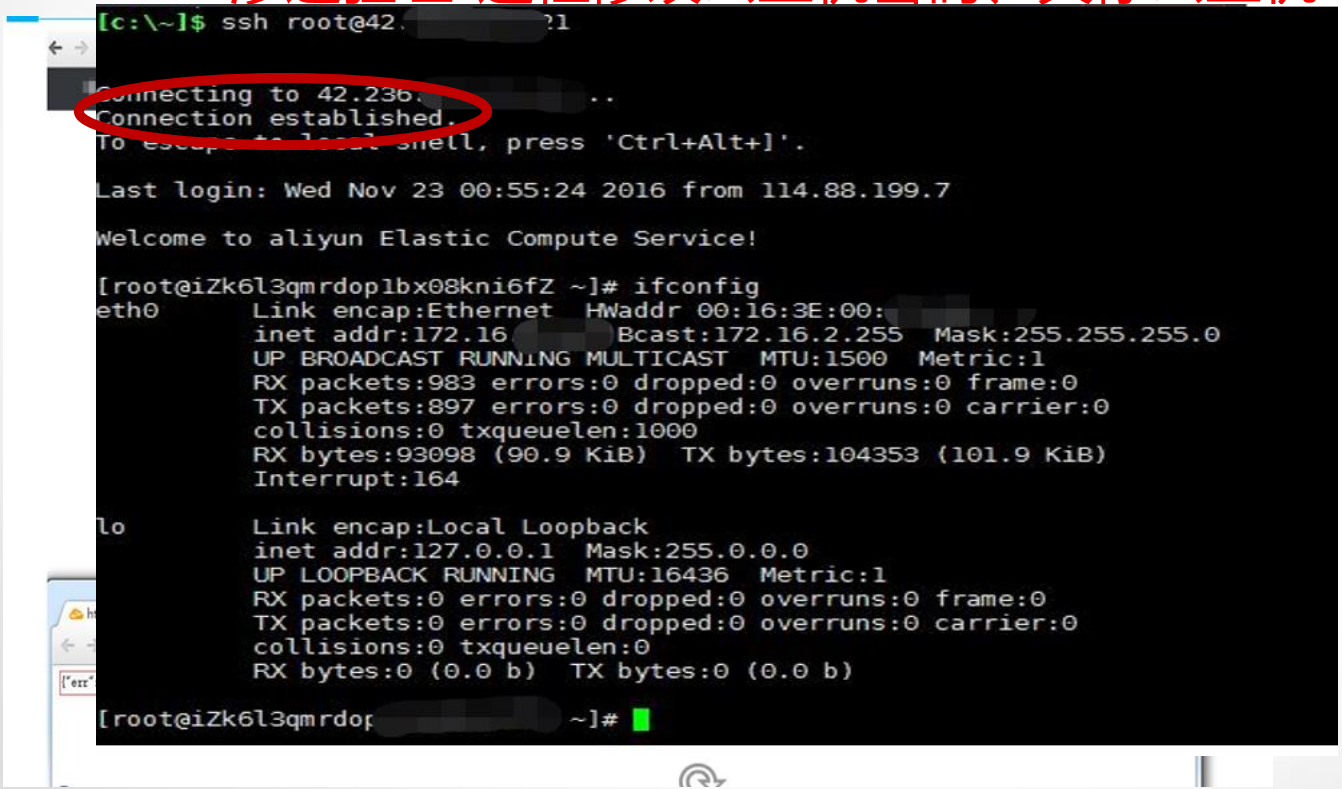
云安全管理问题

云安全管理不到位带来的安全问题

- 与租户权责划分不清晰，SLA不完善
- 整体安全意识不足
- 对内部人员违规操作监管缺失
- 供应链监管缺失

政务云平台安全问题

渗透验证-远程修改云主机密码、关停云主机



政务云平台安全问题

渗透验证-越权获取大量云租户敏感信息

政务云租户安全问题

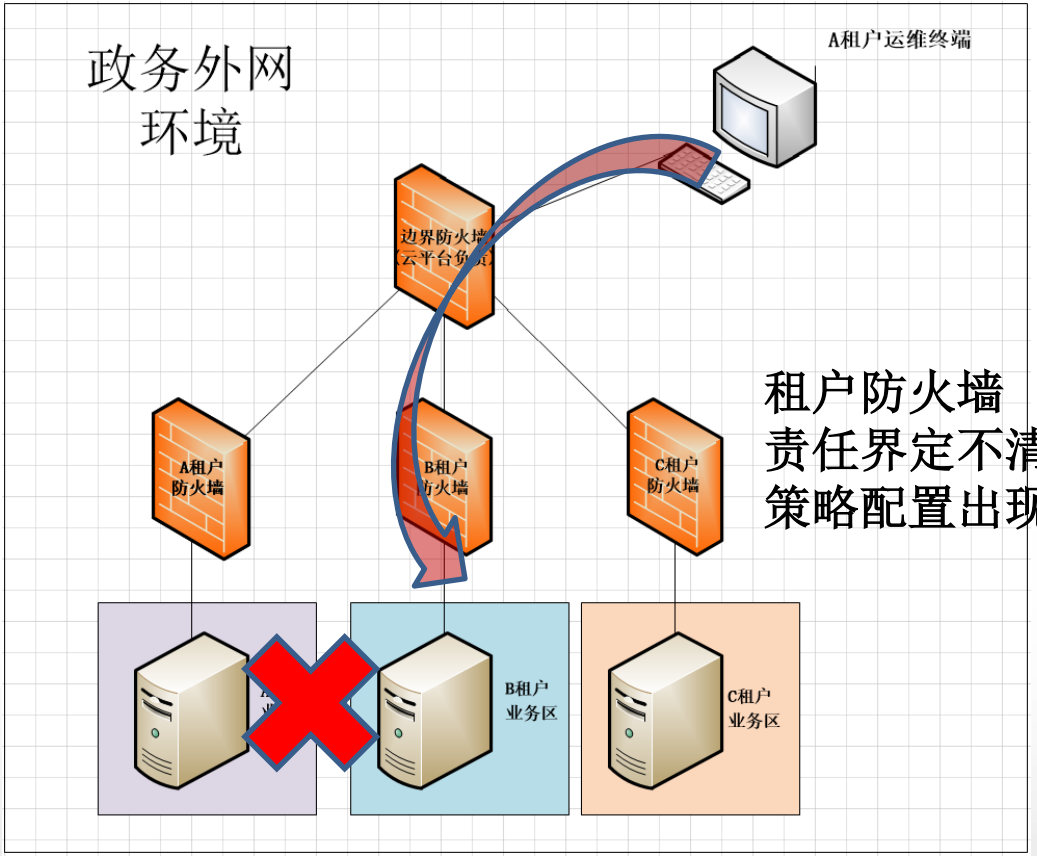
云租户安全防护

- 租户防护不到位，通过自身漏洞被攻击。
- 租户方审计不到位。
- 租户数据在迁移后未及时清除

云安全管理问题

- 安全认知不足
- 未制定数据保护方案
- 与平台方责任界定不清

云租户典型案例



租户防火墙
责任界定不清，
策略配置出现真空。

1 政务云建设管理模式

2 政务云特点及安全挑战

3 政务云安全检测中发现的主要问题

4 政务云安全保障建议

安全保障建议

安全保障建议

结语

无论云平台是新建、在建还是已建成，又或者无论平台采用自主运维、厂商运维还是购买服务的方式，平台和租户的安全都是首先要考虑的问题。

安全是所有“0”前面的那个“1”！

国家信息中心
State Information Center

谢谢！

汇 报 人：尚庆军
时　　间：2018年12月27日