XXXX 云平台数据中心

方案建议书

浪潮集团四川分公司

2015 年 7 月

目录

一、 概述

1.1 项目背景简介

XXX 请根据调研的实际情况填写

1.2 项目需求分析

XXX 请根据调研的实际情况填写

1.3 总体设计原则

XXX 请根据总体规划填写

二、 云中心资源池总体设计规划

整合信息化建设资源，充分利用现有 XXX 市政府中心基础设施，采用云计算技术，结合创新建设模式，搭建标准统一、功能完善、系统稳定、安全可靠、纵横互通、集中统一的 XXX 市政府云计算平台，为各部门信息资源共享、数据交换和系统办公提供良好的支撑。

通过建设 XXX 市云计算平台，方便未来将新增的政府应用快速部署到云计算平台上，大大缩短新 IT 系统的上线时间，预期将节省设备 30%，节约能耗 50%。解决“信息孤岛”，实现信息共享，提高信息安全水平，提升政府监控能力和响应速度，提高工作效率和公共服务水平，提供面向社会的专业性服务和为社会公众提供政务信息服务。通过降低成本、提升效率、节能减排，满足 XXX 市政府要贯彻落实科学发展观，转变发展模式的需要。

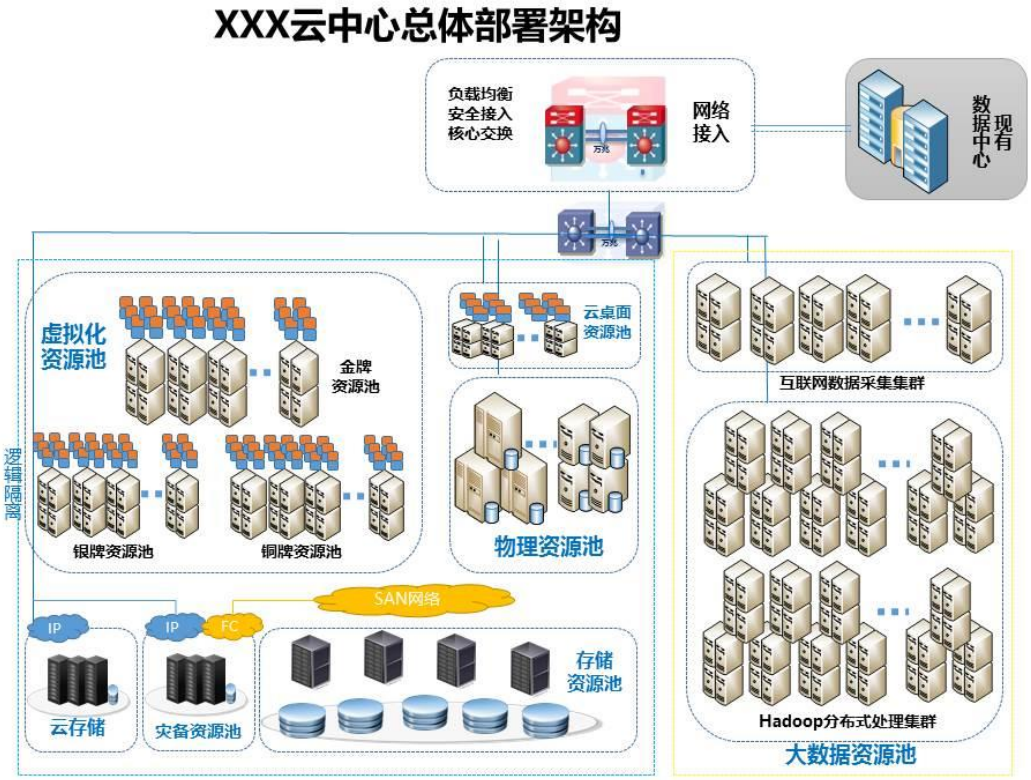
满足在云计算平台上搭建政府的各类应用系统的需要，包括以三层架构为主的应用系统，以及大访问量的应用系统、大数据处理量的应用系统以及大计算量的应用系统。云计算试点业务运行稳定之后，普及和推广云计算模式，将 XXX 市政府部门系统、政府网站应用系统、政务服务业务应用系统、电子监察应用系统等纳入 XXX 市云计算平台，通过建立政府服务事项信息库、办理过程信息库、办理结果信息库、监察规则信息库、监察业务信息库等五个信息库，实现政务服务和电子监察信息资源管理。

XXX 市政府的云计算建设的总体目标是，实现 XXX 市政府系统数据共享，利用云计算弹性、智能、可回收的技术优势，低投资、低能耗、高效率地部署居民健康档案系统、统计直报系统、生猪屠宰监管与溯源系统等与政府职能工作相关

的应用系统。

XXX 市政府的网络、政府网站、业务管理系统、应用及数据服务中心和信息安全保障体系等纳入统一的 XXX 市云计算平台。

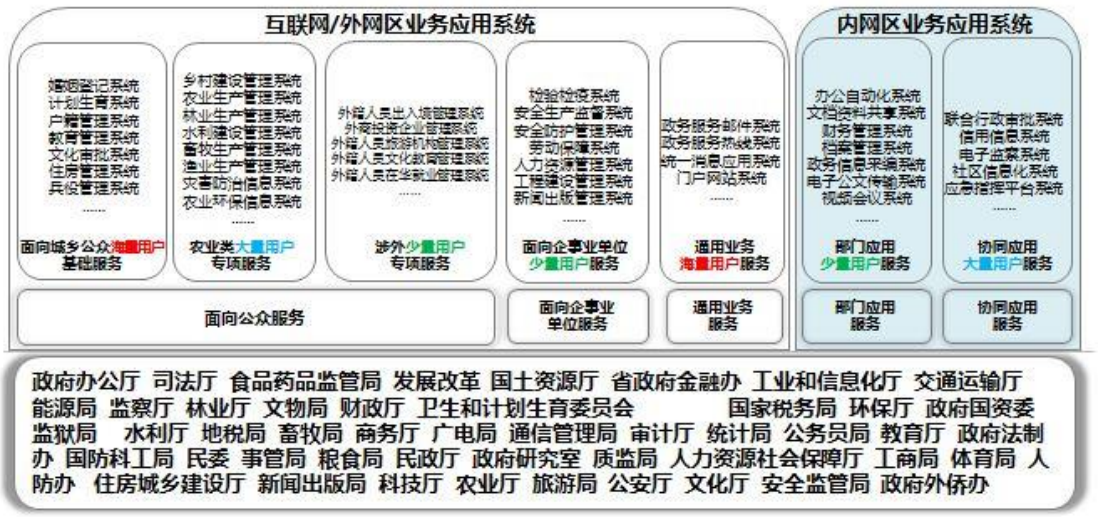
2.1 总体设计思路



在硬件上实现散热、电源、管理功能等非 IT 资源的集中化和模块化，并利用软件虚拟化技术实现计算、存储等 IT 资源的池化和集中管理；将非计算部分的存储、网络等 IO 设备进行池化，机柜内采用高速网络互联，并以软件定义的计算、软件定义的存储和软件定义的网络来满足业务需求，并实现完全的软件定义；将 CPU、内存等所有的 IT 资源完全池化，从硬件上可实现任意组合，根据应用需求智能地分配和组合相关资源，实现完全意义上业务驱动的软件定义数据中心，软件上实现业务驱动和应用感知。

2.2 云平台业务分析

根据本次云平台建设宗旨需要 XXX 市政府主要部门的主要应用都迁移到云平台上进行运行，以下政府各政府单位、事业单位、各组织的主要应用：



根据前期调研和本次规划我们规划了 XXX 市 150 个单位组织的业务上云、数据整合、和应用创新的设计规划。

第三节我们将根据业务的情况对各资源池进行详细的设计和规划。

三、 云平台资源规划设计

云资源主要分为计算资源、内存资源、存储资源、网络资源，云平台安全管理，本项目在充分整合 XXX 市政府数据中心资源的基础上，配置必要软硬件设备，为 XXX 市政府直部门的信息系统提供统一的基础设施服务，在 IaaS 层构建较为完整的 XXX 市云计算平台。建设内容包括以下几部分：

硬件设备：服务器、存储、备份一体机、存储控制系统、SAN 交换机、路由器、交换机、负载均衡、VPN 网关。

软件设备：物理服务器和虚拟服务器的操作系统、虚拟化软件、中间件、大型数据库系统、云计算管理平台。

安全系统：防火墙、入侵防御、防毒墙、网页防篡改、身份认证系统、运维安全审计系统、数据库安全审计系统、漏洞扫描系统。同时采购专业机构提供的云安全服务等。

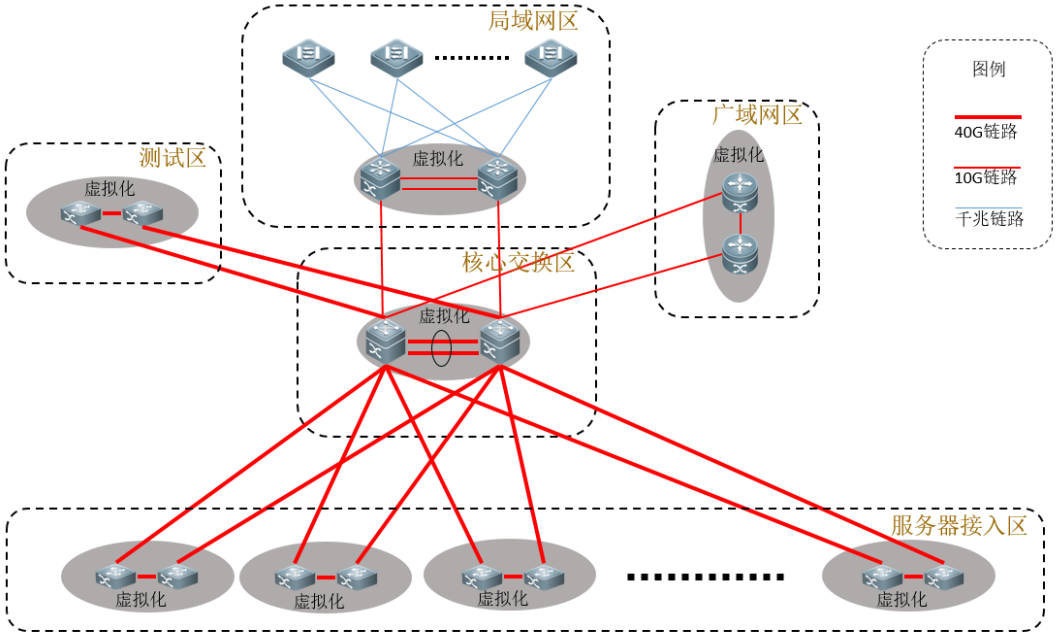
机房配套设备：UPS、精密空调、标准机架。

3.1 网络资源规划

网络是连接所有数据中心 IT 组件的通用实体，构建坚实的网络基础设施将为数据中心业务永续、管理与运维提供基础保障。

3.1.1 云数据中心网络整体规划

XXX 市云数据中心网络设计中，我们建议采用端到端网络设计原则，为数据中心进行分区、分层和分级设计。在考虑现有业务系统、服务器资源、存储资源的情况下，数据中心改造可参考如下设计的拓扑图进行网络建设：



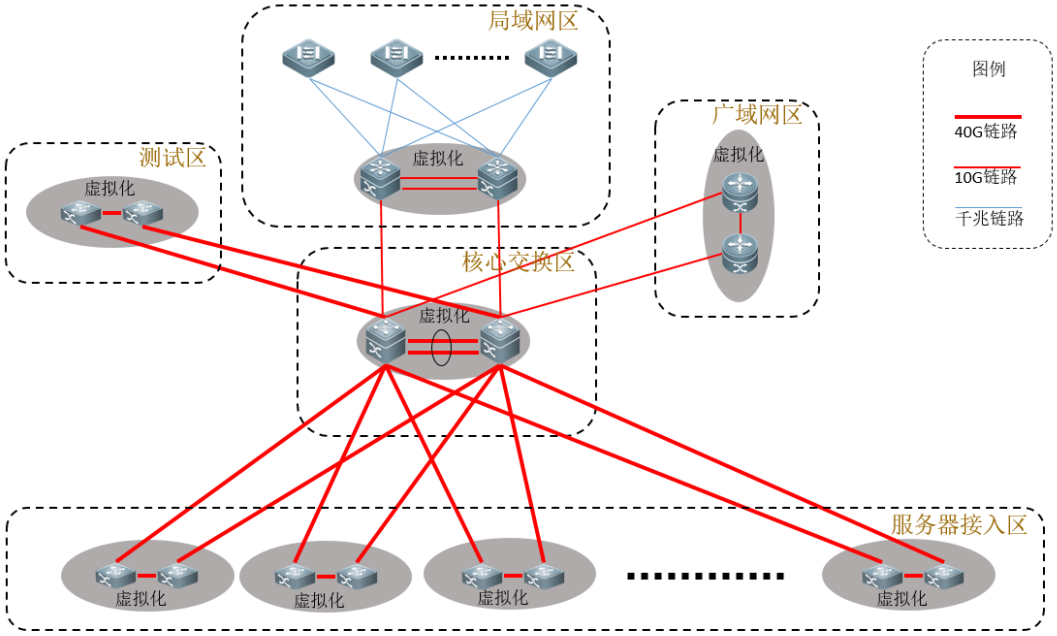
方案中采用两层结构设计构建一个高速转发的网络基础平台。全网采用两台核心交换机作为云数据中心平台的网络核心，负责整个云数据中心平台的数据转发。并且通过 2 条互联的 40G 链路采用虚拟化技术将两台核心设备虚拟化为一台逻辑设备有效实现网络的高可靠性。核心交换机与数据中心万兆接入交换机采用 40G 链路互联。

方案中，在服务器接入层部署数据中心万兆接入交换机，所有服务器均通过 2 条万兆链路分别与 2 台数据中心接入交换机相连；且该两台数据中心万兆接入交换机通过互联的 40G 链路采用虚拟化技术将两台接入设备虚拟化为一台逻辑设备从而有效实现从网络接入到核心的高可靠性，同时两台数据中心交换机各通过 1 条 40G 链路上联核心交换机，两条 40G 链路可进行捆绑，实现高达 80G 的高速数据转发通道。

此次规划的云数据中心中所采用的核心交换机、数据中心万兆接入交换机均支持数据中心特性：如虚拟化技术、VEPA（虚拟以太网端口聚合，IEEE 标准）、FCOE、DCB 等。为数据中心的将来的更复杂的业务开展提供技术支撑。

3.1.2 云数据中心网络分层设计

XXX 云数据中心网络架构采用模块化分层、分区的规划模式。各个功能区域之间逻辑互联和功能区域内部分层次，如下图：



从数据中心功能出发，网络架构按不同的功能采用分区结构。根据各部分功能，数据中心分为：**核心交换区、服务器接入区、局域网区、广域网区、测试区**。通过分层、分区的模块化规划，能够支持整体网络结构的扩展；标准化每个服务分区的网络规范，简化网络的运行、管理。

3.1.3 核心交换区规划

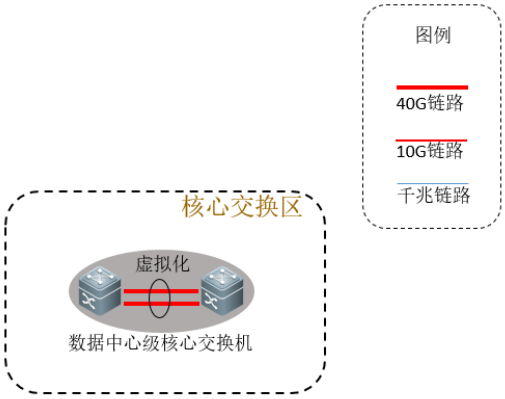
核心交换设备的选择

核心交换区作为XXX云数据中心平台的核心区域，主要负责连通所有的功能分区，构建一个高速交换的以太网骨干网络。

网络中心节点作为局域网络系统的心脏，必须提供全线速的数据交换，当网

络流量较大时,对关键业务的服务质量提供保障。另外作为整个网络的交换中心,在保证高性能、无阻塞交换的同时,还必须保证稳定可靠的运行,所以核心层交换机本身提供多种冗余如管理模块/电源/风扇等关键模块支持冗余。同时,作为网络核心节点还需要具有良好的可扩充性和高密度端口的承载能力,能够保障随着将来数据中心规模的扩充而平滑升级。

核心交换区作为连接各个区域的核心层,采用具有冗余架构和配置的2台机架式数据中心级交换机,并通过两条40G链路互联,使用虚拟化技术,将两台核心交换机虚拟为一台,以简化拓扑,实现毫秒级的故障恢复。两台核心设备通过一体化板卡的扩充实现统一的数据表项、统一的管理地址、统一的设备配置等单台逻辑设备的对外特征。



虚拟化技术不仅使2台核心交换设备简化成一台逻辑核心层设备,同时网络各层之间的多条链路连接也将变成两台逻辑设备之间的直连,因此可以将多条物理链路进行跨设备的链路聚合,从而变成了一条逻辑链路,增加带宽的同时也避免了由多条物理链路引起的环路问题。如下图所示,将接入与核心交换机两两虚拟化,层与层之间采用跨设备链路捆绑方式互联,整网物理拓扑没有变化,但逻辑拓扑上变成了树状结构,以太帧沿拓扑树转发,不存在二层环路,且带宽利用

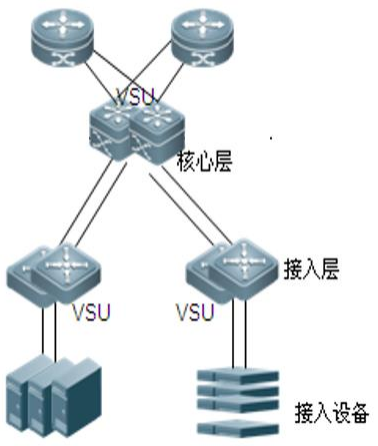
率最高。

此时其它交换机到核心交换机的双链路上联，等同于双链路连接到1台核心上，能够实现跨设备链路聚合。当上联1条链路中断时，相当于是聚合链路的一条成员链路出现故障，切换到另一条成员链路的时间是10到20毫秒。极端情况下，即使其中一台核心机宕机，也不会对全网造成大的影响。甚至能够保证整个切换过程的用户业务切换无感知。两台交换机组成虚拟化集群以后，管理员可以实现对两台交换机统一管理，而不需要分别连接到两台交换机分别进行配置和管理。从而简化了管理流程。

和传统网络相比，虚拟化的优势有：**1、简化组网拓扑结构，简化管理，2、减少了设备数量，减少管理工作量，3、多台设备合并后可以有效的提高性能，4、多台设备之间可以实现无缝切换，有效提高网络HA性能。**

核心交换区可靠性考虑

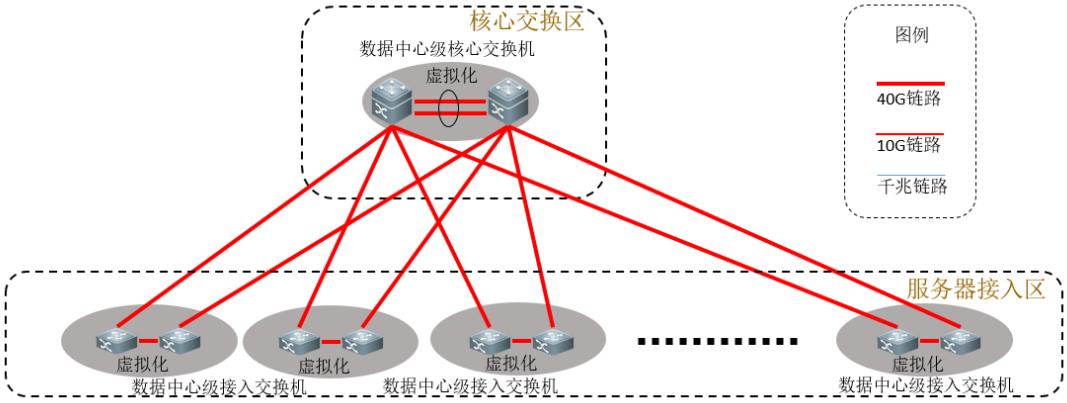
网络可靠性由设备冗余、链路冗余来保证。为便于虚拟机的迁移，核心层与服务器接入层交换机之间需要采用二层网络进行互联，这样就需要解决接入层和核心层之间二层流量的环路问题。现在一般推荐使用基于 VSU 的无环网络方案，不再使用传统的 STP ＋VRRP 方案。具体如下：



核心采用两台框式交换机集群。接入层采用盒式交换机，盒式交换机每两台VSU。接入层交换机和核心交换机间的链路进行链路聚合。

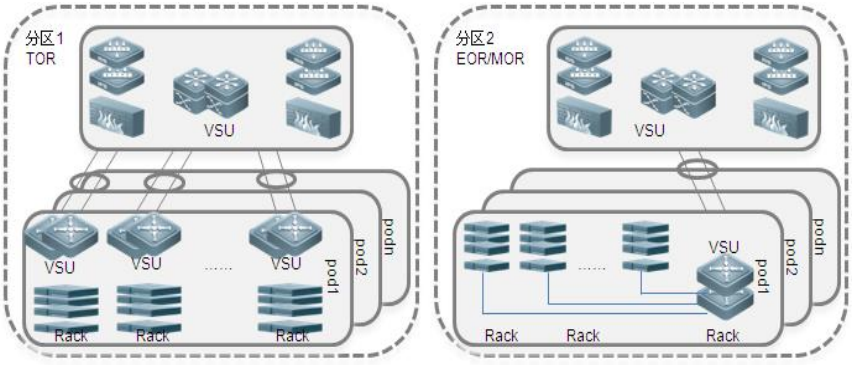
这个方案有如下优势：1、简化管理和配置：首先，VSU 技术将需要管理的设备节点减少一半以上。 其次，组网变得简洁，不需要配置 STP/REUP/VRRP 等的协议。2、快速的故障收敛：链路故障收敛时间可控制在<50ms ，大大降低了网络链路/设备故障对业务的影响。3、带宽利用率高：采用链路聚合的方式，带宽利用率可以达到 100%。4、扩容方便：当进行网络升级时，只需要增加新设备既可，不需要更改网络配置，平滑扩容，很好的保护了投资。5、提高可靠性：以单链路故障率为 1 小时/1 千小时为例，增加到两条链路，就可以将故障率降低到 3.6 秒/1 千小时（两链路均故障的概率为（1 小时/1 千小时）*（1 小时/1 千小时），等于 3.6 秒/1 千小时）。6、可靠性的另一个重要方面是设备可靠性，核心区设备一般为框式设备，**在可靠性方面的要求包括**：1、主控单元的备份；2、交换网板的备份； 3、支持电源模块的备份； 4、需要提供模块化的风扇设计，支持单风扇失效； 5、支持所有模块的热插拔；6、支持 CPU 防攻击； 7、需要提供完善的各种告警功能。

服务器接入区设计



EOR/TOR 规划

接入层交换机部署在服务器机架内或者独立的网络机柜中，部署在服务器机架内的一般称为 TOR （Top Of Rack），部署在列头柜中的一般称为 EOR （End Of Row），一般提供二层交换功能。



TOR 的部署模式一般适合高密度的机架服务器的接入;EOR 模式一般适合低密度的服务器，如小型机的接入。两者的区别如下表所示：

部署方式	TOR	EOR/MOR（Middle Of Rack）
服务器类型	1RU 机架服务器	2-4RU 机架服务器、刀片服务器、小型机
服务器数据	15-30 台	8-12 台
适合场景	高密度服务器机柜	低密度服务器机柜和网络机柜
布线	简化服务器机柜与网络机柜间布线	布线复杂
维护	接入设备多，管理维护复杂，电缆维护简单，扩展性好	接入设备少，维护简单电缆维护复杂

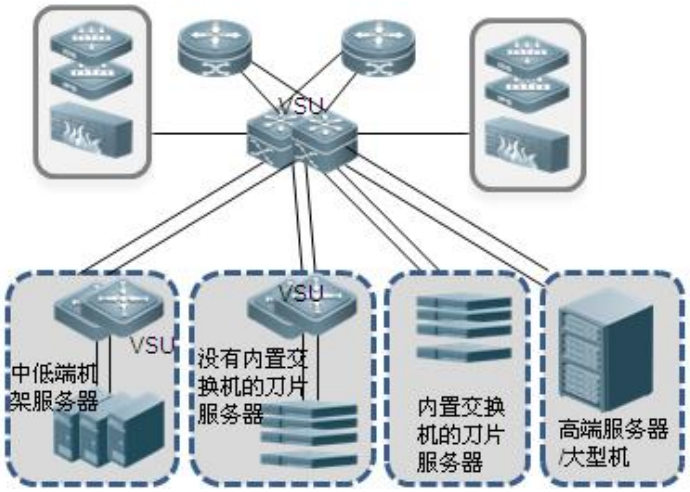
服务器的接入方式分为下面四种情况：

1、中低端机架服务器，数量众多，通过接入层交换机接入。

2、高端服务器/大型机，数量较少且重要性高，直接接在核心交换机上，保证带宽。

3、没有内置交换机的刀片服务器，通过接入层交换机接入。

4、内置交换机的刀片服务器，直接接在核心交换机上，减少交换网络的层级，提升网络性能。



服务器接入区可靠性考虑

服务器分区的可靠性包括网络可靠性、网络设备可靠性和服务器接入网络的可靠性：

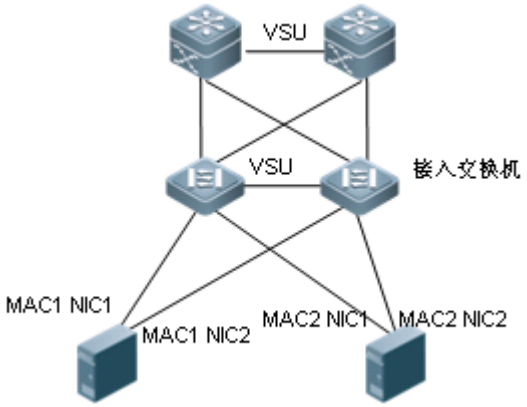
1、网络可靠性通过 VSU 或堆叠的无环网络提供，具体见核心区可靠性规划。

2、网络设备可靠性采用交换机 VSU 或堆叠。

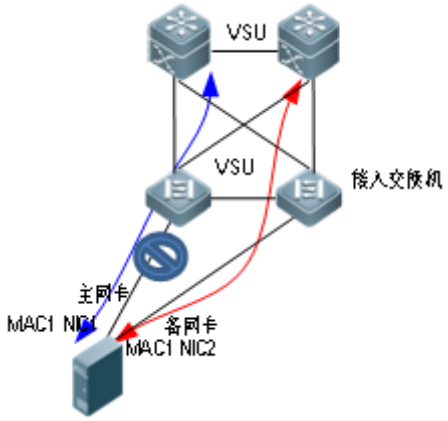
3、服务器接入网络可靠性是通过服务器双网卡来支持。

服务器网络驱动程序将两个网卡捆绑成一个虚拟的网卡，对外提供一个唯一的 IP 地址。需要服务器支持网卡聚合特性（NIC Teaming）：当一个网卡失效，另一个网卡接管它的 MAC 地址。两个网卡采用主备或者负载分担的方式。

1、双网卡主备方式： 对于主备方式的双网卡，两个网卡的 MAC 相同（如下图，都是 MAC1）。服务器在发现主网卡故障后，切换到备网卡。并通过备网卡发出免费 ARP。网络设备必须正确处理这个免费 ARP 报文，才能将发给服务器的流量切换到新的转发路径上。



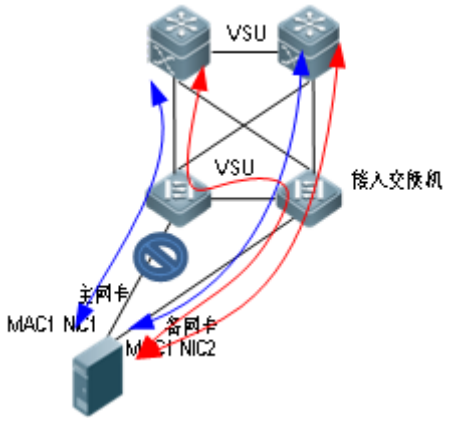
如下图所示，主网卡故障后，转发路径需要从蓝色曲线切换到红色曲线。因此，接入层交换机在处理免费 ARP 报文时，需要将 MAC1 的出接口刷新到连接备网卡的链路上，因此要求接入层交换机配置时将对应服务器主备网卡的两个端口配置在同一个 VLAN ，不配置成链路捆绑(否则不会刷新 MAC1 的出接口)。



核心层交换机在处理免费 ARP 报文时，由于核心交换机和接入层交换机之间的是多条链路捆绑成的 AP 链路，因此，核心/汇聚层交换机不会感知到变化。

2、双网卡负载分担方式：对于负载分担方式的双网卡，两个网卡的 MAC 相同（如下图，都是 MAC2），而且两个网卡都可以发送和接收流量。接入层交换机必须配置成虚拟化模式，并将对应服务器主备网卡的两个端口配置成链路捆绑。才能屏蔽 MAC 地址在两个交换机端口间不断“跳跃”的处理。

如下图所示，没有故障时转发路径时蓝色曲线，两个网卡都有流量。左边网卡故障后，转发路径需要从蓝色曲线切换到红色曲线。



由于核心层交换机和接入层交换机之间的是多条链路捆绑成的 AP 链路，因此，核心层交换机感知不到接入层的变化，仍然会将流量发给左边的接入层交换机。这个流量通过接入层交换机之间的 VSU 链路转发给右边的接入层交换机，由右边的接入层交换机转发给服务器。

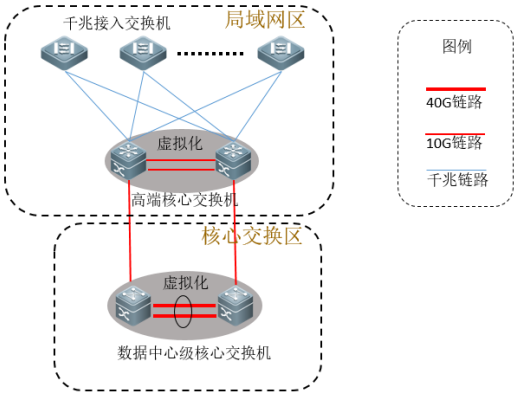
万兆接入、40G 上联核心设计

云数据中心的服务器接入区主要由各个功能分区的交换机组成，提供各个分区内部服务器的接入。为保证高性能的数据传输，数据中心接入层交换机采用高密度万兆接口设计，通过万兆接口与服务器进行互联保证数据中心的数据高速转发。

每组配备 2 台具备 40G 上行的接入交换机，同时具备高背板带宽和包转发率的设备。在可靠性上每个交换机通过双 40G 链路接入核心交换机，同时进行链路捆绑，实现虚拟集群，确保链路可靠性。同时两台接入交换机之间通过一个 40G 链路互联，并构成虚拟化的数据和控制信息传输通道。

局域网（管理、维护）区设计

XXX 云数据中心平台局域网一方面用于 E 华路公司内部工作人员接入，实现对数据中心平台的管理、维护。同时还提供其他其它辅助业务功能模块的接入，如认证服务器、安全策略设备的接入等。



局域网区的网络建设，建议采用 2 台高端机架式交换机作为局域网的核心交换机（如果经费紧张，也可只采用 1 台全冗余配置的高端机架式交换机），通过虚拟化技术虚拟化为 1 台逻辑交换机，然后通过 2 条捆绑的万兆链路，实现与云数据中心平台的核心交换机互联。

局域网核心交换机与云数据中心平台核心交换机之间的互联可采用基于 2 条万兆捆绑链路的三层互联。并可在互联通道间部署相应的安全设备，实现网络数据交互的安全、可控。

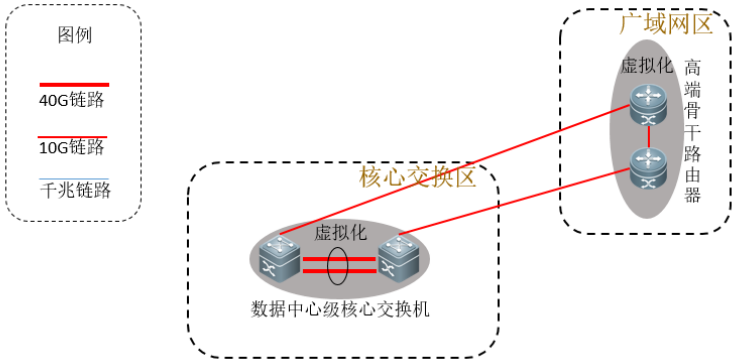
辅助业务服务器可直接连接到局域网核心交换机上。对于可靠性要求高的辅助业务服务器，其连接方式可参考云数据中心平台的服务器与接入交换机之间的连接方式。

XXX 云数据中心内部工作人员的接入可通过在局域网核心交换机下挂载接入交换机来实现。可采用千兆接入、万兆上联的高性能接入交换机，也可采用千

兆接入、千兆上联（或捆绑多条千兆链路上联）的普通全千兆交换机来实现。

广域网区设计

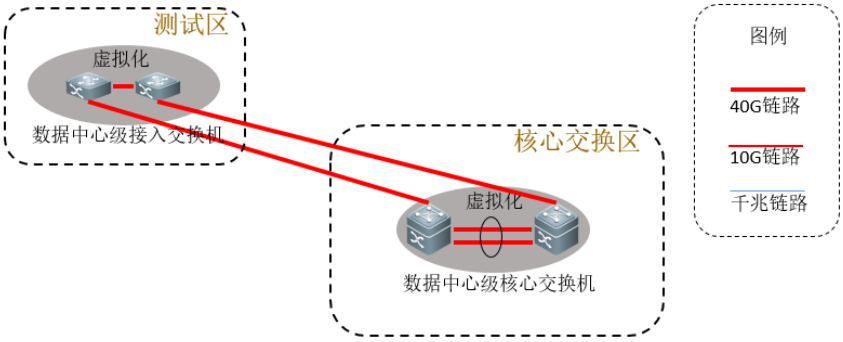
广域网接入区是 XXX 市各委办局接入云数据中心平台的接口。广域网区部署两台高端广域网路由器，形成设备和链路的双备份设计，并启用 MPLS VPN 功能，实现与各接入单位之间的连接。



测试区

测试区是接入云计算中心平台的业务开发、测试系统。测试系统是准上线业务系统，提供业务系统上线前对本地系统业务和压力测试。当测试通过时，管理人员可直接将业务系统直接转接到服务器接入区进行上线。

测试区部署 2 台与服务器接入区相同的万兆接入 40G 上联的高性能盒式交换机，以提供与服务器接入交换区相似的网络功能和性能。同时还应在测试区与云数据中心平台核心交换机的互联通道处部署相应的安全设备，以保障测试环境的偶发性不可预计问题所造成的对正常业务系统的影响。



3.2 云服务器资源规划

XXX 市政府直属各部门地应用有数据库应用、大访问量应用系统如政府门户网站、对外小访问量 Web 网站，根据他们对服务器性能要求高低不一样分别设计为金牌资源池、银牌资源池、铜牌资源池。

3.2.1 服务器 CPU 资源规划

数据库-金牌 CPU 资源池

数据库是信息系统政府单位重要组成部分，是数据处理与信息管理系统的核心。数据库解决了计算机信息处理过程中大量数据有效地组织和存储的问题，在数据库系统中能够减少数据存储冗余、实现数据共享、保障数据安全以及高效地检索数据和处理数据。

XXX 市政府直属各部门预计 150 个,每个部门按照部署 1 个数据库服务器搭建为利用虚拟化软件的 HA 的确保安全，所以我们需要规划总共 150 个虚拟机的金牌资源池。为保证各部门的数据库设计都能满足峰值时间的应用，所以我们将以 OLTP 业务类数据库方式来计算机 CPU 需求配置。

对于 OLTP 业务类数据库系统，其服务器计算能力一般可以使用 TPCC 测算公式进行测算：数据库服务器计算能力需求 TPCC(Tpmc)值=∑(M1 * M2)/(1 - M3)，

M1 为每分钟业务事务量，M2 为标准事务量比率，为一个当前业务系统联机事务相当于多少个标准 tpmC 事务值，一般 M2 取值应该在 5-15 范围内，M3 为系统资源冗余率，一般取 20%-40%。

XXX 市总人口为 323.58 万人，根据调研同时在线使用政府办公系统处理业务的人不到 1‰，而这 1‰的人同时使用同样的业务和同样数据的几率为 20%，所以同时在线等并发人数约为 648。

根据以上方式可以知道该数据库系统的业务事务，主要来自审批工作平台的业务请求，根据调研估算得到数据库工作平台系统并发用户数峰值约为 648，根据经验每个审批业务事务相当于 4-10 个标准 Tpcc 事务，根据上述 TPCC 计算公式可以计算出纳税服务一体化审批工作平台数据库系统 TPCC（Tpmc）约为：

TPCC（Tpmc）= (648 * 10)/(1 - 30%) ≈ 926；另外数据库的日志缓存，日志缓冲数据库的用户请求来自审批业务系统 队列服务器，因此数据库计算能力需求类似，取相同 TPCC 值 926，所以单个政府的数据库虚拟机需要满足 1852Tpmc 性能值，按照 Tpmc 的对比处理去要 4 核 2.0GHZ 的 CPU 来处理这些并发需求，按照虚拟化服务器转换率 70%-92%,预留 30%作为故障迁移资源，在预留 20%作为新上系统测试资源，所以总体需要 CPU 的资源为：150*4*2.0GHZ/70%/(1 - 30%)/(1 - 20%)≈3062GHZ，按照浪潮 TS860 配置 8 颗 12 核心 Intel E7-8857 v2 3.0GHZ 总共需要 11 台，以满足 XXX 市政府直属部门的数据库应用。

应用服务器-银牌 CPU 资源池

应用服务器是承载着不同应用的网上任务的单点登录和权限管理等功能，为登录人提供统一访问平台，主要对外不同的业务，本周 XXX 市云平台为 XXX

市直属部门规划 10 个应用平台，这部分资源对性能要求不是太高所以我们需要 1500 个银牌 CPU 资源池。

XXX 市总人口为 323.58 万人，根据调研同时在线使用政府办公系统处理业务的人不到 1‰，而这 1‰的人同时使用同样的业务和同样数据的几率为 20%，所以同时在线等并发人数约为 648。

WEB 用户并发需求测算可以按照国际公测组织参照 SPECweb2005 的评测标准，Web 应用服务性能需求：WEB 应用服务器 SPEC Web2005 值= (总用户数 * 在线率 * 在线用户平均发起 http 请求数)/ (1-冗余率)= (648*20%*4)(1-30%)

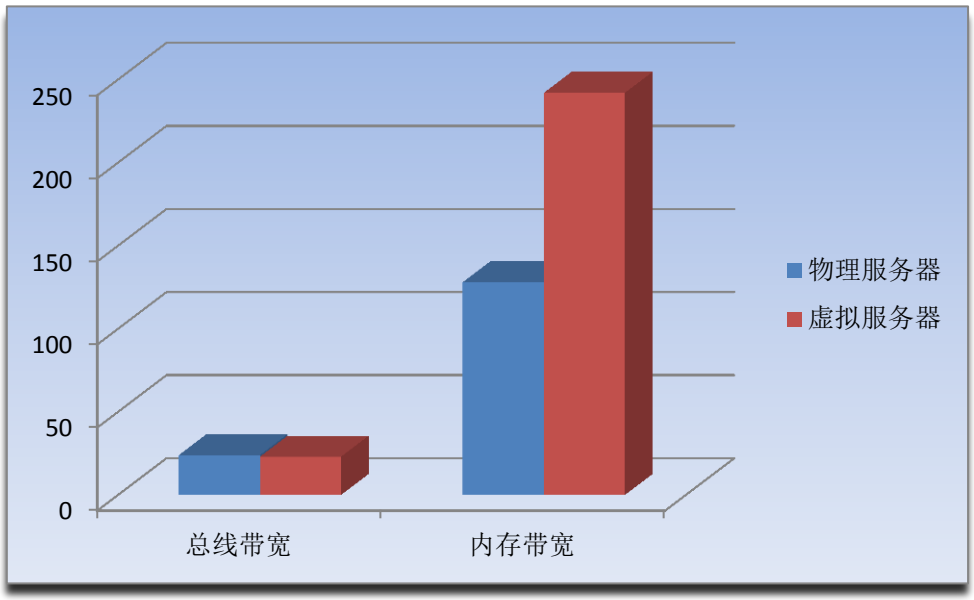
= 740，按照 CPU 的并发处理性能要求我们 1 核 1.0GHZ 就可以满足。按照虚拟化服务器转换率 70%-92%,预留 30%作为故障迁移资源，在预留 20%作为新上系统测试资源，所以总体需要 CPU 的资源为：150*10*1*1.0GHZ/70%/(1 - 30%)/(1 - 20%)≈3827GHZ，按照浪潮 NF8460 配置 4 颗 12 核心 Intel E7-4850 v2 2.3GHZ 总共需要 34 台，以满足 XXX 市政府直属部门的应用服务器需求。

管理服务器-铜牌 CPU 资源池

为云平台、安全平台，作业平台搭建统一的管理资源池，按照 100 个管理服务器计算，每个管理服务器配置 1 核 1.0GHZ 就可以满足，按照虚拟化服务器转换率 70%-92%,预留 30%作为故障迁移资源，在预留 20%作为新上系统测试资源，所以总体需要 CPU 的资源为：100*1*1.0GHZ/70%/(1 - 30%)/(1 - 20%)≈256GHZ，按照浪潮 NF5270M4 配置 2 颗 10 核心 Intel E5-2650 v3 2.3GHZ 总共需要 6 台，以满足 XXX 市政云管理中心管理服务器资源需求。

3.2.2 服务器内存资源规划

采用虚拟机在内存性能的对比物理机上结果比较惊喜，除了内存延迟之外其他，其他数值例如总线带宽与物理服务器几乎没有差别，而在内存带宽的性能上有将近 1 倍左右的性能优势，这同样的得益于虚拟平台底层优秀的硬件平台基础，这样证明在在虚拟服务器上同等配置应用或数据库更不容易发生因内存溢出或错误引起的停用故障。（内存延迟在带宽同等的状况下，对性能的影响基本可以忽略）



数据库-金牌内存资源池

根据数据的最佳实践要求至少按照每数据库 8GB 的配置，虚拟化对内存的转化率为 92%到 95%，预留 30%作为故障迁移资源，在预留 20%作为新上系统测试资源，XXX 市政府直属单位总共需要内存资源为：150*64GB/92%/(1 - 30%)/(1 - 20%)≈2330GB，按照 11 台 TS860 计算机每台至少需要配置 256GB 的内存容量。

应用服务器-银牌内存资源池

根据应用服务器最佳实践要求至少按照每数据库 1GB 的配置，虚拟化对内存的转化率为 92%到 95%，预留 30%作为故障迁移资源，在预留 20%作为新上系统测试资源，XXX 市政府直属单位总共需要内存资源为：150*10*1GB/92%/(1 - 30%)/(1 - 20%)≈2912GB，按照 34 台 NF8460M3 计算机每台至少需要配置 128GB 的内存容量。

管理服务器-铜牌内存资源池

根据应用服务器最佳实践要求至少按照每数据库 2GB 的配置，虚拟化对内存的转化率为 92%到 95%，预留 30%作为故障迁移资源，在预留 20%作为新上系统测试资源，XXX 市政府直属单位总共需要内存资源为：100**2GB/92%/(1 - 30%)/(1 - 20%)≈389GB，按照 6 台 NF5270M4 计算机每台至少需要配置 64GB 的内存容量。

3.2.3 服务器网络资源规划

传统的网络规划设计依据高可靠思路，形成了冗余复杂的网状网结构，结构化网状网的物理拓扑在保持高可靠、故障容错、提升性能上有着极好的优势，是通用设计规则。云计算的大规模运营，给传统网络架构和传统应用部署都带来了挑战，新一代网络支撑这种巨型的计算服务，不论是技术革新还是架构变化，都需要服务于云计算的核心要求，动态、弹性、灵活，并实现网络部署的简捷化。具体来说传统网络面临的挑战主要有以下几点：

传统网络的复杂性在实际的运维中，管理人员承担了极其繁冗的工作量；

云计算平台下多虚拟机部署在同一台物理服务器上运，服务器的利用率从 20%提高到 80%，服务器端口流量大幅提升，对网络性能提出更高要求；

云计算平台中，虚拟机在物理服务器之间进行迁移，为了避免虚拟机迁移后路由的震荡和修改网络规划，迁移通常只在在二层域进行，因此云计算平台需要具备一个性能更高、二层域更大的网络环境为迁移提供保障。

通过分析云计算对传统网络基础架构带来的挑战，我们可以从两个方面来应对。一是通过构建高性能、高可靠的网络，从而满足云计算给网络带来的压力；二是通过构建虚拟化网络来满足云计算中由于虚拟机部署、迁移、以及安全策略实施对网络提出的灵活性、安全性的要求。

数据库-金牌网络资源池，应用服务器-银牌网络资源池，管理服务器-铜牌网络资源池，都按照以下规划

网络段描述	主机物理网卡	IP 地址分配
管理网络	千兆 NIC01 和 NIC02	管理 IP 地址
vMotion 网络	千兆 NIC03 和 NIC4	独立 IP 地址
业务网络	万兆 NIC01 和 NIC2 万兆 NIC03 和 NIC4	数据网 IP 网络

以上设计保证了整个虚拟化平台的网络链路冗余，不同网段的业务系统在虚拟环境中能够正常工作，达到虚拟化整合的预期效果。

3.3 云存储资源规划

XXX 市云数据中心的建设，涉及到存储资源的整合，存储平台承载了所有的宝贵的政府资料和数据、虚拟机系统数据等，所以所选择的存储平台必须首先具备高可靠的设计，保障业务 7×24 小时不中断；其次，存储平台必须具备高性能，充分满足高业务压力需求，保障科研应用系统流畅运行；另外，存储平台必须智能化，可以动态的调整资源，自动调优，优化 I/O 处理，同时要有良好的

兼容性,需要同虚拟化软件进行联动,完成虚拟机相关操作,提供系统整体性能;再者，存储平台要具备良好的可持续扩展能力，满足业务未来几年发展需求。但由于 XXX 市政府直属单位中不同的应用对存储的要求也不一样，有的需要高性能和高 IOPS 的存储资源池，有的对性能无太大要求只是需要海量的存储空间，建议此情况，同样将存储资源池分为金牌存储资源池、银牌存储资源池、铜牌存储资源池,同时为达到非结构化的数据和文件类型的数据同时存储在统一的存储平台所以要求使用 SAN+NAS 统一的存储。我们将从存储的 IOPS 性能、存储的带宽 Throughput，容灾备份性能方面进行分析。

3.3.1 存储性能 IOPS 规划

根据 XXX 市直属单位的业务类型主要为数据库、应用服务器、和管理服务器，这三类按照数据库 150 个，应用服务器 1500 个，管理服务器 100 个来考虑，存储的 IOPS 也应该逐一考虑。按照之前计算最大并发为 648 人每个应用，每个人按照 1 个业务计算,最大业务峰值 648 笔/小时,最大峰值 10% 在同一时刻产生，648* 10%≈65 笔/秒，平均每笔交易产生按照平均 10 个 IO 读写估计，由此可以计算出每个应用最大峰值为 65* 10=650 IOPS，所以我们总共的 IOPS 规划为 1750*650≈1137500 个 IOPS。

3.3.2 存储带宽规划

XXX 是云平台里所有应用平均按照读 8KB，写 4KB，总体 1137500iops，读写比 8：2 计算，平台峰值写带宽=8KB*1137500*0.7+4KB*1137500*0.3≈7.5G;根据一个 8Gb 的光纤主机通道，所能支撑的最大流量应当是 8Gb=800MB／s 的理

论值，实际流量在传输光纤协议的时候只有 70%-90%的转化率，所以一个 8Gb 的实际可以达到 560MB/s，所以我们需要 14 个 8Gb 光纤口来传输数据才能满足云平台应用，另外需要考虑 2 个 8Gb 的光纤接口作为后续容灾备份规划。

3.3.3 存储容量规划

XXX 是云平台里由于业务类型不一样所有我们在容量上按照金牌存储资源池、银牌存储资源池、铜牌存储资源池，来规划。

金牌存储资源池

按照每个数据库 20GB 容量规划，我们需要 150*20=3000GB 的高性能盘，每年数据库增长 80%计算,按照系统 3 年数据量计算总体数据量为 3000GB+2400GB×3 年=10200GB,还需要留出 50%的快照空间 100%的数据缓存交互数据库空间，以及 50%的预留空间,可以计算出 3 年总需要 10200×(1+0.5+1+0.5)=30600GB，这部分按照高性能的 SSD 资源池，按照每块 800GB 容量，以 RAID5 的方式做安全保护，所以我们一共需要 48 块 800GB SSD 硬盘。

银牌存储资源池

按照每个应用 10GB 容量规划，我们需要 1500*10=15000GB 的高性能盘，每年数据库增长 20%计算，按照系统 3 年数据量计算总体数据量为 15000GB+3000GB×3 年=24000GB，还需要留出 50%的快照空间 100%的数据缓存交互数据库空间，以及 50%的预留空间，可以计算出 3 年总需要 24000×（1+0.5+1+0.5）=72000GB，这部分按照性能要求不高的 SAS 资源池，按照每块 800GB 容量，以 RAID5 的方式做安全保护，所以我们一共需要 96 块 900GB SAS 硬盘。

铜牌存储资源池

XXX 市政府直属单位的应用中有很多经常不使用的冷数据，或者非结构化数据,这部分对性能要求不高,但对容量要求极大,按照每个应用 80GB 容量规划，我们需要 1750*80=140000GB 的高性能盘，每年数据库增长 50%计算，按照系统 3 年数据量计算总体数据量为 140000GB+70000GB×3 年=350000GB，这部分按照性能要求不高的低价的 NL-SAS 资源池，按照每块 4TB 容量，以 RAID5 的方式做安全保护，所以我们一共需要 96 块 4TB NL SAS 硬盘。

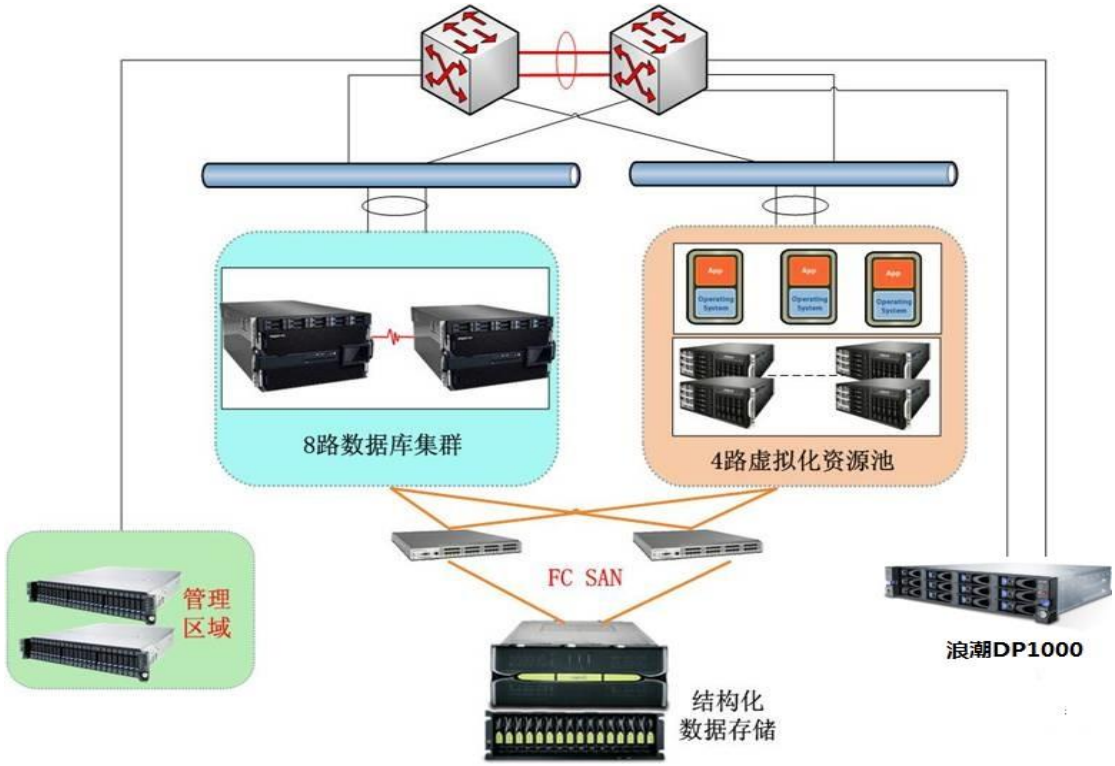
3.3.4 存储总体规划

综上所述，按照性能、带宽、容量、已经容灾需求考虑，我们需要一台含有 4 控制器的高性能的 SAN+NAS 的存储,所以推荐浪潮 AS8000-M2 配置 4 控制器，256GB 高速缓存，16 个 8GB 光纤接口，配置独立的前数据的压缩卡，配置 48 块 800GB SSD 硬盘,配置 96 块 900GB 10K 转速 SAS 硬盘,配置 96 块 4TB NL SAS 7.2K 硬盘，配置自动层软件，配置精简配置软件，配置数据快照软件，配置原远程镜像软件。

3.4 数据备份机制规划

云计算中心，虚拟化平台虚拟机应用业务日益激增，40.8%以上的企业已部署虚拟化应用，21%的用户计划在 1 年内规划，虚拟应用平台导致核心数据丢失性日益严重，主要针对客户大量的虚拟化平台数据做备份，虚拟机带来了独特的备份难题，大量重复数据产生，数据所需的时间不断增加，为客户推荐备份一体机重删功能，提高重复数据备份效率。虚拟机数据量超过 20T。既然备份策略能

抵御用户错误和某些情况下的软硬件故障，比较长的恢复时间和多恢复点是能被接受的。



按照 XXX 市云计算中心目前数据量情况，备份一体机规划为 100TB 以上，所以建议使用浪潮 DP1000-M1 配置 100TB 的备份容量许可，含所有的数据库，应用，虚拟化备份许可。

3.5 云管理平台规划设计

云计算管理平台包括云资源管理平台、云连营管理平台、网络管理平台。云资源管理平台包括 IT 基础架构中的物理资源和虚拟资源的管理，其中虚拟计算资源的管理集成厂商的云平台;云运营管理平台含业务管理模块和运营管理模块。

云计算管理平台总体架构如下:

3.5.1 云管理平台架构

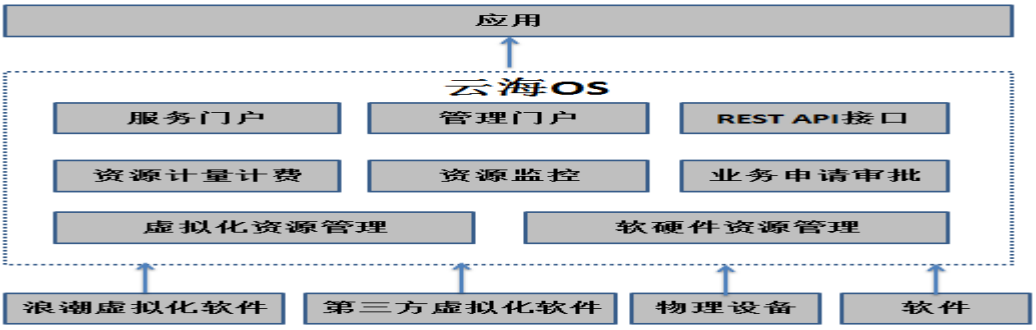
云设施即服务(IaaS，Cloud Infrastructure as a Service)：系统供应商可以向用户提供同颗粒度的可度量的计算、存储、网络和单机操作系统等基础资源，用户可以在之上部署或运行各种软件，包括客户操作系统和应用业务。

云平台即服务 (PaaS，Cloud Platform as a Service)：云计算平台供应商将业务软件的开发环境、运行环境作为一种服务，通过互联网提交给用户。云平台即服务，需要构建在云基础设施之上。用户可以在云平台供应商提供的开发环境下创建自己业务应用，而且可以直接在云平台的运行环境中上运营自己的业务。

云软件即服务(SaaS，Cloud Software as a Service)：运营商通过互联网，向用户提供软件服务的一种软件应用模式。传统的 SaaS 与云 SaaS，在客户体验上基本类似，如新浪邮箱和 Gmail 邮箱，客户感受是类似的。但传统的 SaaS 直接构建在硬件设备之上,不能实现后台资源的多租户共享,也无法实现资源的动态流转,实际并不属于云计算的范畴。云 SaaS，要求这些软件业务运行在云平台服务层或构建在云基础设施层之上。云 SaaS 的优势，体现在后台资源的动态伸缩和流转上，资源可扩展性更强，这一重大优势是传统 SaaS 所不具备的。

本方案中云计算平台由资源池、虚拟化平台、云管理平台组成。资源池部分主要有物理设备组成，包括服务器，存储和网络等基础架构资源，通过虚拟化平台对基础架构设备进行池化，从而形成资源池；虚拟化平台就是将物理资源进行池化的软件组合；云计算管理平台就是对底层资源池和虚拟化软件进行管理，并且，针对管理和运维需要，云计算管理平台实现云计算服务的交付和云计算中心用户和流程的管理以及数据中心的监控。

浪潮 ICM 数据中心管理软件，秉承开放、模块化、标准化的设计理念，支持多种异构虚拟化平台，实现虚拟化数据中心的智能化运维，实现基础设施的服务化。

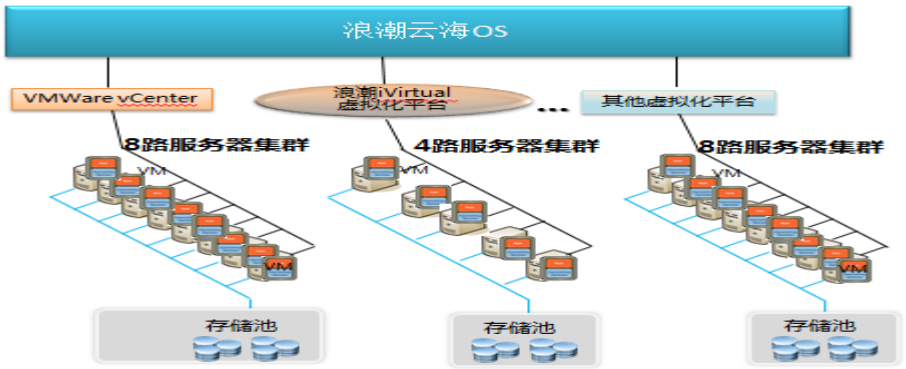


浪潮浪潮 ICM(云海 OS)，可兼容浪潮服务器虚拟化软件 iVirtual 及 VMWare 等第三方虚拟化软件，可直接管理物理设备（包括服务器、存储设备、网络设备

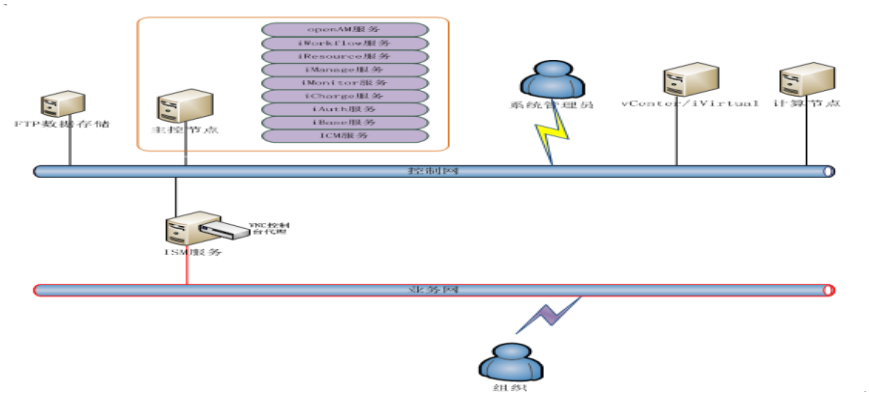
等），实现数据中心各类软硬件资源的管理及监控，可将虚拟资源作为服务提供给用户使用，实现资源使用精准的计量计费。云海 OS 对外提供所有功能组件的 REST API 接口，可与客户原有系统做集成，第三方厂商可基于此做定制化开发。

3.5.2 云软件部署架构

云海 OS 支持对多种异构虚拟化平台的集中管理，如图所示：



云海 OS 支持单网和多网两种部署方式，单网部署适用于仅包含单一网络的简单网络环境，比如研发专网、测试专网等，如图所示；多网部署适用于复杂的网络环境，即网络环境中包含业务网、管理网等多类网络，各类网络之间可实现物理隔离，如图所示。



组件	组件描述	组件基本配置

主控节点	云海 OS 的控制中心节点，是系统管理员对数据中心资源的管理接口，可部署在物理服务器上，也可部署在虚拟机上。	操作系统版本为：CentOS 6.0 X86_64；最低配置：4 核 CPU、8GB 内存，双网卡，位于管理网络。
ISM 服务节点	云海 OS 的自服务管理节点，组织及组织用户可通过访问 ISM 服务节点，申请及使用资源，可部署在物理服务器上，也可部署在虚拟机上。	操作系统版本为：CentOS 6.0 X86_64；最低配置：4 核 CPU、4GB 内存，双网卡，同时连接业务网络以及管理网络，需要安装 VNC 控制台代理。
VNC 控制台代理	用于 VNC 控制台转发、信道加密。可单独部署在一台服务器节点上，也可以部署在 ISM 服务节点上	操作系统版本为：CentOS 6.0 X86_64，需要开启 SSH 服务，同时连接业务网络以及管理网络
虚拟化管理节点	底层的虚拟化管理中心，支持 VMWare vSphere 及浪潮 iVirtual 等多种虚拟化平台	Inspur iVirtual 为最新版本即可，位于管理网络。
FTP 数据存储	云海 OS 的二级存储，用于存放系统管理员、组织管理员及组织用户上传的 ISO 镜像文件以及虚拟机、应用服务模板文件。	配置 NFS，最好拥有大容量磁盘空间，位于管理网络
计算节点	云海 OS 的虚拟化节点，当前支持 VMWare ESXi 及 Inspur Xen 两种。	没有具体的配置要求
管理网	云海 OS 内部管理节点所在的网络，	

	专用于管理节点内各服务之间的控制指令的传递以及管理节点与自服务节点之间通信指令的传递。	
业务网	云海 OS 用户使用虚拟机控制台时所使用的网络，专用于虚拟机内部用户业务数据的传递。	

3.5.3 资产管理

产品功能	功能描述
资源池管理	通过添加虚拟控制中心(例如 VMWare vCenter 等)将多个异构资源池整合成一个更大的资源池，进行统一管理和资源分配。资源池管理包括对资源池的扩充和缩减，暂停使用某些资源池等操作。
资源池集群管理	集群是资源的载体，是资源池的组成单位。通过集群管理实现为不同用户提供不同等级的资源服务，扩充或缩减资源池容量，可重新导入资源池的新增集群，也可暂停在某些集群上新建虚拟数据中心及应用服务，可查看集群内的主机及所挂载存储的信息

存储池管理	云海 OS 支持对集群所挂载的存储池的管理，包括查看存储的状态、地址、存储总量、已分配容量、实际剩余容量等信息
虚拟数据中心管理	虚拟数据中心(vDC)界定了组织能够使用资源的范围，组织管理员可将 vDC 资源分配给组织内用户。虚拟数据中心管理包括创建、导入，修改配置等操作。
虚拟网络管理	虚拟网络允许组织及组织用户像定义物理网络一样定义组织自己内部的网络，以及与组织外网络的连接方式，包括直连、NAT 等，组织网络的地址分配、VLAN 划分等。

应用服务管理	应用服务(vApp)是指提供某种服务的一个或多个通过特定网络连接在一起的虚拟机集合。可通过服务模板、新建虚拟机 2 种方式创建应用服务。操作包括新建、开启、关闭、重启、删除、复制、修改、更改所有者、导出为模板等操作。
	
虚拟机管理	单独对组成 vApp 的虚拟机操作。功能包括操作虚拟机控制台、开启、关闭、重启、挂起、恢复、删除、复制、移动、更改虚拟机，插入或弹出 CD/DVD,将虚拟机导出为模板，创建及恢复虚拟机快照等操作。
	
模板&镜像管理	将虚拟机模板、应用服务模板或操作系统安装镜像上传并导入到服务目录下，用于部署虚拟机、应用服务和安装操作系统，也可将模板和镜像文件共享给其他组织使用。

3.5.4 云平台业务管理

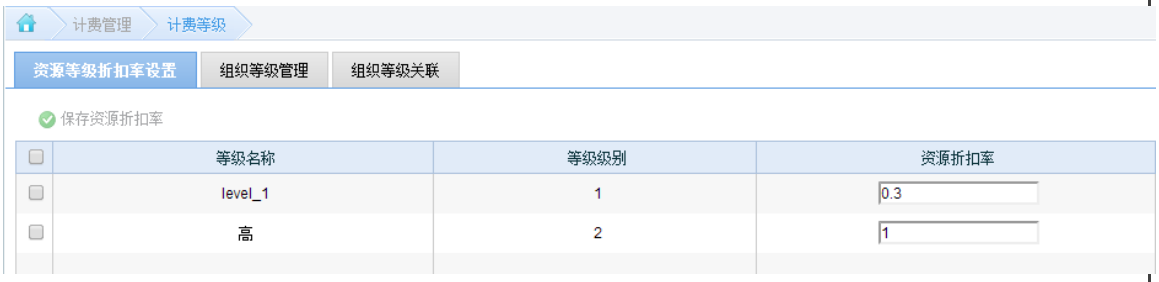
产品功能	功能描述
业务流程管理	审批流程引擎实现虚拟数据中心、组织网络、应用服务、虚拟机审批流程的自定义。
	
业务申请	组织管理员可向系统管理员申请虚拟数据中心、组织网络，组织用户可向组织管理员申请应用服务、虚拟机
	
业务审批	审批用户提交的虚拟数据中心(vDC)、组织网络、应用服务(vApp)、虚拟机申请

审批历史查询	查询每个订单的详细信息，包括订单内容，申请人、申请时间等。

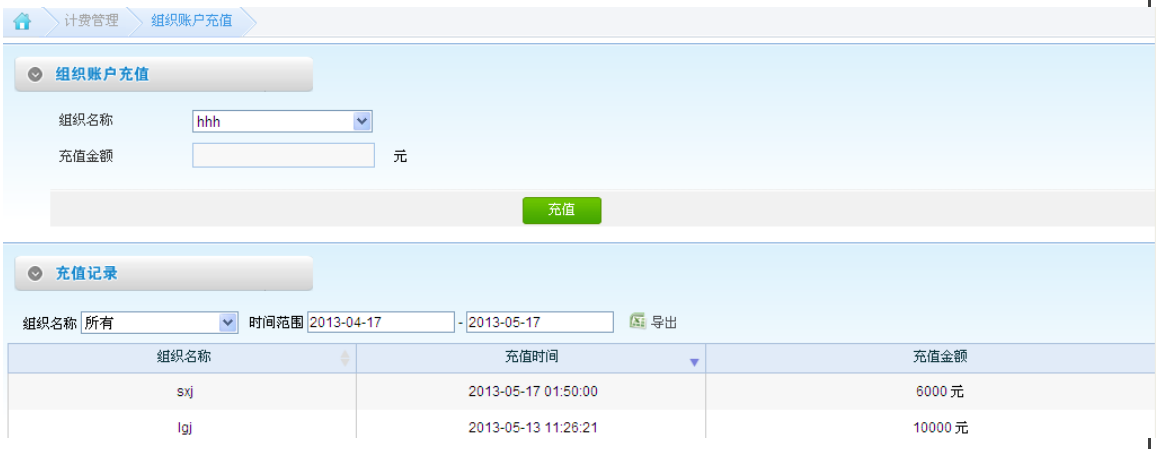
3.5.5 云平台计费管理

产品功能	功能描述
计费设置	设置用户帐户余额的提醒周期及提醒方式（邮件、短信）；定义资源单价（元/资源度量单位/小时）；欠费处理方式等

计费等级管理	资源按一定标准分为不同的等级，各等级的资源计费系数不同；组织也分为不同的等级，不同等级的组织计费系数也不同；系统可自行设置资源等级、组织等级对应的折扣率，从而为不同的用户提供不同的计费系数



组织账户充值	为组织账户充值，并可查询充值历史。



查询组织账户余额	查询各组织的帐户余额。

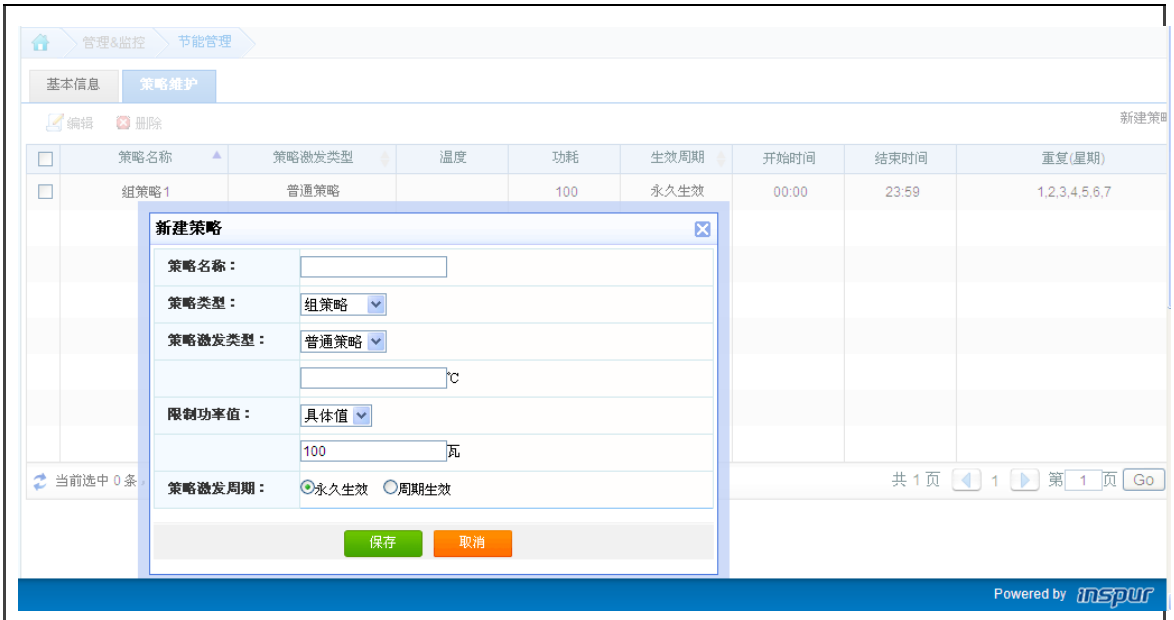
查询组织账单	查询组织每月的消费金额及费用明细。

3.5.6 云平台监控管理

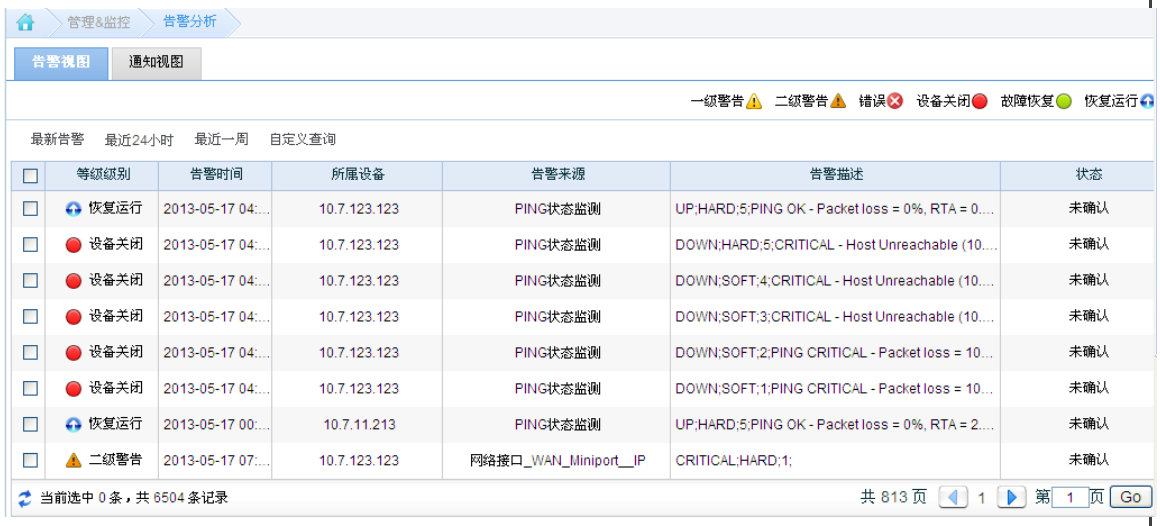
产品功能	功能描述
资源监控	监控服务器、网络设备等物理资源，数据库、操作系统、web 服务等软件资源以及虚拟化系统的性能及状态，并以图表的形式展现。

资源管理	对服务器进行远程开关机操作以及 BMC 配置管理；获取并显示服务器、存储设备、网络设备、数据库、操作系统、web 服务、虚拟化系统的基本信息、性能及状态信息

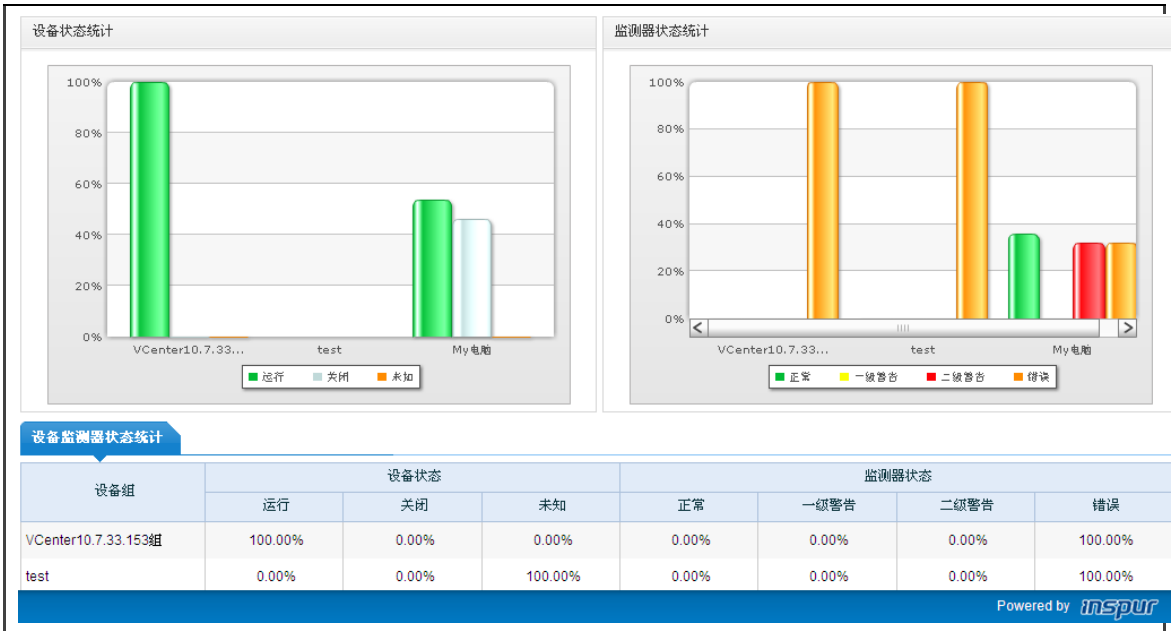
节能管理	节能管理在不影响正常业务的情况下，通过降低服务器 CPU 频率来降低服务器组或服务器的能耗。功能包括节能策略制定及服务器组或服务器的能耗曲线显示。



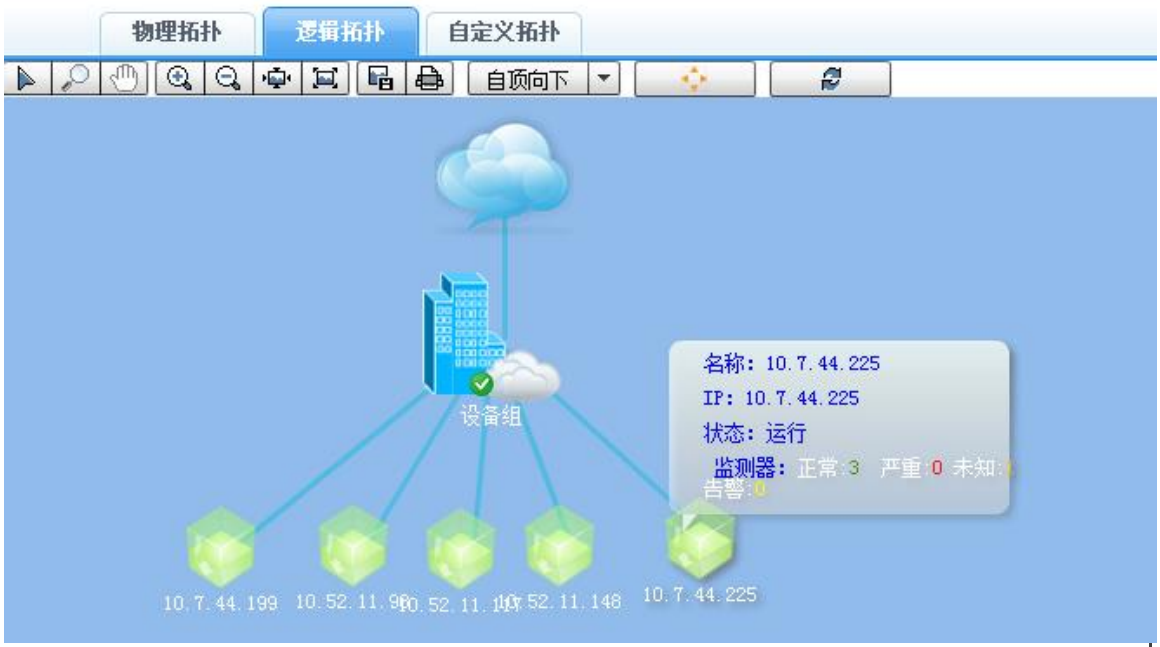
告警分析	分时段显示所监控的各类软硬件资源的异常告警信息，告警的处理、告警通知的发送等



报表中心	提供所监控的各类软硬件资源状态统计、性能统计报表

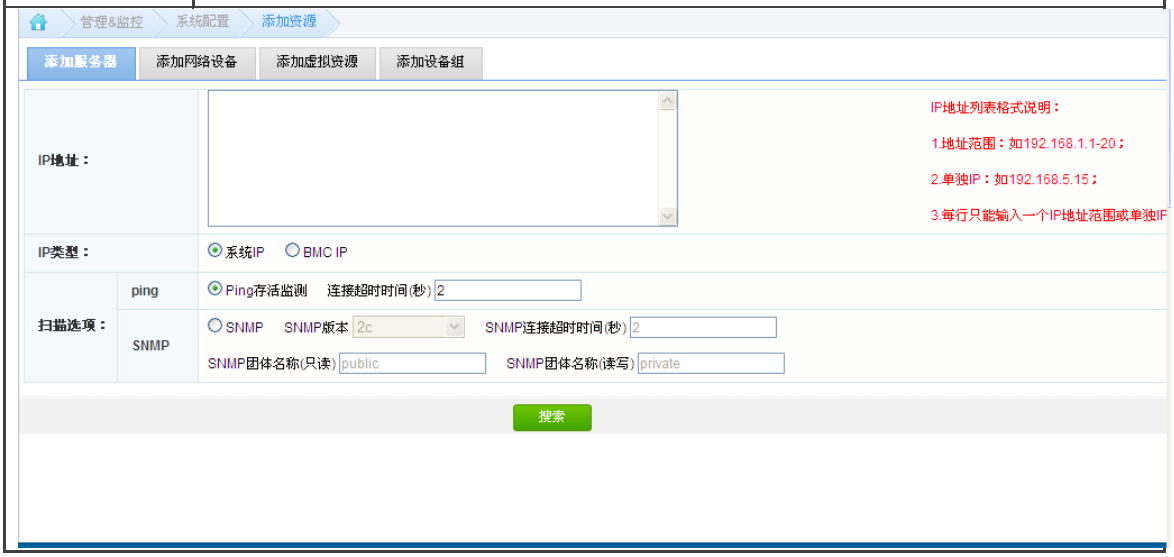


拓扑视图	拓扑显示系统中设备的物理连接视图、逻辑分组视图，支持用户自定义拓扑，根据业务依赖绘制业务拓扑；拓扑图上动态显示对象的实时监控信息系统。



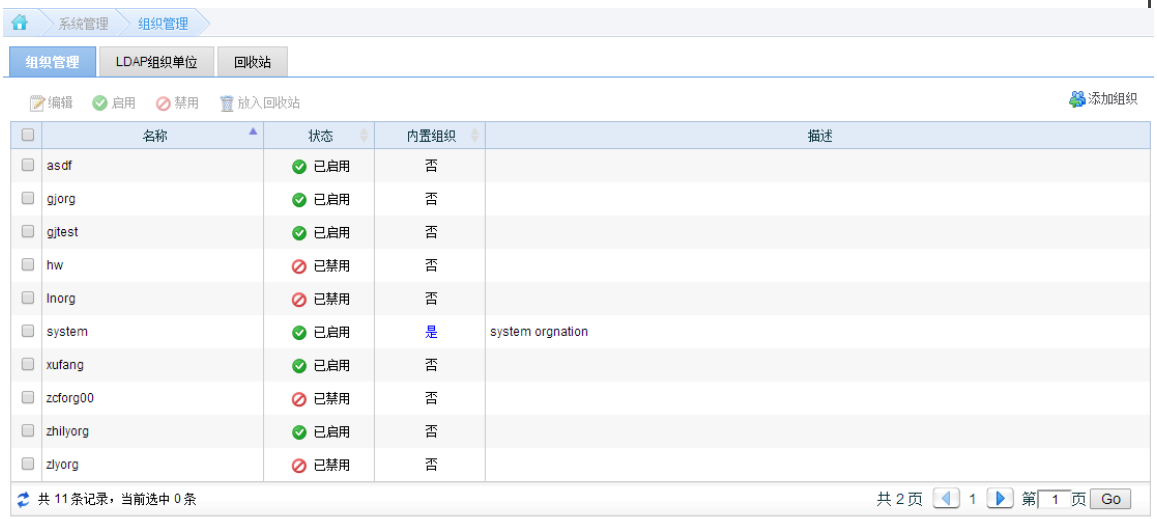
系统配置	监控管理模块的基础性配置。如添加资源，为资源添加监测项，通知时间表设置，告警通知联系人设置，备份与恢复当前的监控管理配置信息等,系统提供 ping ，tracert，snmpWalk，checkTcp，ipmiTool

	等小工具进行网络测试



3.5.7 云平台系统管理

产品功能	功能描述
组织管理	组织是用户的集合，是虚拟数据中心（vDC）及 vApp 的所有者，也是资源使用费用的承担者。组织管理功能包括添加组织、编辑、启用、禁用、删除等操作，可指定某 LDAP 用户目录作为组织的用户来源。



用户管理	系统管理员管理各组织的组织管理员，各组织管理员管理其组织内

	部的组织用户。用户管理包括：添加新用户、从 LDAP 导入用户，修改用户基本信息、重置密码、启用、禁用、解锁、删除等操作。

用户名	全名	状态	组织	角色	类型	是否失连	是否锁定	用户目录	电子邮件	电话	描述
1	linan	已启用	lnorg	组织用户	本地用户	--	否	--	linanlinan@in...	12345123	1
2	adsfj	已启用	lnorg	12	本地用户	--	否	--	asdf@asdf.as	12345678	2
7	7	已启用	zz	组织管理员	LDAP	否	否	ou=test03,dc=...			
admin	admin	已启用	system	系统管理员	本地用户	--	否	--	wangchx@ins...	15066109690	
audit	audit	已启用	system	审计管理员	本地用户	--	否	--	shaoxj@insp...	15275127213	
gj	guojing	已启用	gjorg	组织管理员	本地用户	--	否	--	guojing@insp...	1234567890	
guojing	guojing	已启用	gjorg	组织用户	本地用户	--	否	--	guojing@insp...	435765897890	

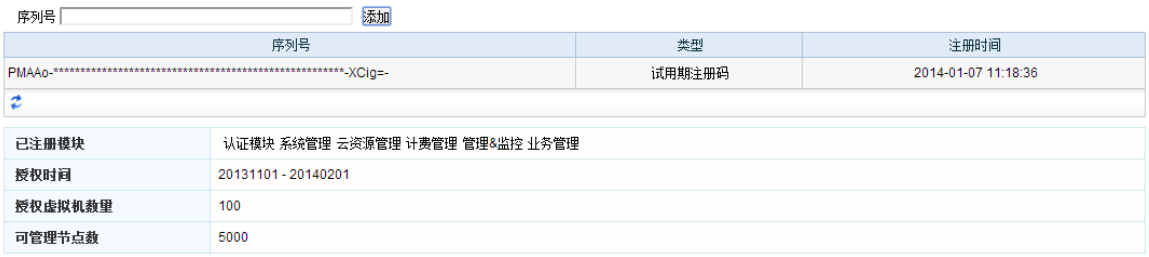
角色管理	角色是系统操作的集合，界定了相同角色的用户拥有的操作权限范围。云海 OS 除支持 4 个内置角色（系统管理员、审计管理员、组织管理员、组织用户）外，还支持用户自定义角色。

名称	内置角色	角色类型	描述
newrole	否	系统管理员	
审计管理员	是	审计管理员	审计管理员
系统管理员	是	系统管理员	
组织用户	是	组织用户	
组织管理员	是	组织管理员	

日志管理	审计管理员负责日志的管理工作，包括日志管理参数的设置，日志的导出与删除；系统的其他用户可根据时间、组织、用户、操作对象、操作结果、所属模块等条件查询相关的操作记录。

系统设置	设置系统发送提醒、告警等通知的邮件、短信参数；设置用户登录系统的最大错误登录次数及锁定时长；设置不允许登录系统的客户端 IP 黑名单

序列号管理	序列号分为正式序列号和试用期序列号，序列号到期后，系统将无法使用，需重新注册。序列号限定了可使用的功能模块，可同时开启的虚拟机数量及可监控的物理设备节点数量。



LDAP 管理	云海 OS 可与用户现有的 LDAP 系统集成，实现基于 LDAP 的身份验证访问机制，LDAP 的用户可作为云海 OS 的用户来管理和使用资源。

3.6 云平台安全规划设计

XXX 市智慧城市大数据中心网络信息系统安全保障建设的基本思路是：以保护信息系统为核心，严格参考等级保护的思路和标准，从多个层面进行建设，满足 XXX 市智慧城市大数据中心信息系统在网络层面、系统层面、应用层面、系统运维管理层面的安全需求，建成后的保障体系将充分符合国家标准，能够为 XXX 市智慧城市大数据中心业务的开展提供有力保障。

本方案针对 XXX 市智慧城市大数据中心网络环境和应用系统为基础，分析 XXX 市智慧城市大数据中心的网络安全建设需求，结合国家等级保护的建设规范和技术要求而编制，为 XXX 市智慧城市大数据中心网络信息安全的等保符合性建设提供指导。

3.6.1 网络安全设计

等级保护中对网络访问控制的要求

根据对 XXX 市智慧城市大数据中心应用系统安全保护等级达到**安全等级保护三级** S3A2G3 的基本要求，进行网络访问控制技术和产品的实施过程中，必须符合以下技术要求：

访问控制（G3）：

1、 应在网络边界部署访问控制设备，启用访问控制功能；

2、 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；

3、 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

4、 应在会话处于非活跃一定时间或会话结束后终止网络连接；

5、 应限制网络最大流量数及网络连接数；

6、 重要网段应采取技术手段防止地址欺骗；

7、 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

8、 应限制具有拨号访问权限的用户数量。

等级保护中对网络访问控制的实现

实现以上控制要求的最有效方法就是在 XXX 市智慧城市大数据中心的网络关键网络位置部署应用防火墙网关设备，本次项目建议在互联网边界以及业务关联单位边界分别部署应用防火墙。

网络入侵防护

根据对 XXX 市智慧城市大数据中心应用系统安全保护等级达到**安全等级保护三级** S3A2G3 的基本要求，进行网络入侵防范产品和技术实施过程中，必须符合以下技术要求：

入侵防范（G3）

1、 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门

攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

2、 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

等级保护中对网络入侵防护的实现

对于 XXX 市智慧城市大数据中心的业务系统安全防护，重点要实现区域边界处入侵和攻击行为的检测，因此需要互联网区域部署 IPS 设备以及 WAF 等安全设备。

安全审计

根据对 XXX 市智慧城市大数据中心应用系统安全保护等级达到**安全等级保护三级** S3A2G3 的基本要求，进行网络入侵防范产品和技术实施过程中，必须符合以下技术要求：

安全审计（G3）

1、 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

2、 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3、 应能够根据记录数据进行分析，并生成审计报表；

4、 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；

等级保护对网络安全审计的实现

信息安全审计管理是运维管理最重要的一部分，被审计对象不仅仅包括服务区域中的应用服务器等，还要对终端的行为进行审计；此外重要网络设备和安全

设备也需要列为审计和保护的对象。

需要在 XXX 市智慧城市大数据中心网络的核心交换机上部署 IDS 入侵检测系统以及数据库审计系统，将核心交换机对应的端口流量镜像到对应设备上，对抓到的包进行分析、匹配、统计，从而实现网络安全审计功能。

3.6.2 主机安全设计

等级保护中对主机恶意代码防范的技术要求

根据对 XXX 市智慧城市大数据中心 OA 等系统安全保护等级达到**安全等级保护三级** S3A2G3 的基本要求，进行系统主机恶意代码防范技术实施过程中，必须要符合以下技术要求:

恶意代码防范（G3)：

1、 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

2、 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

3、 应支持防恶意代码的统一管理。

等级保护对主机防恶意代码的实现

根据以上要求,XXX 市智慧城市大数据中心网络服务器系统和终端防病毒系统应具备自动更新病毒代码库的功能，具备统一的病毒代码控制台。可部署一套网络防病毒软件。

网络防病毒体系一般由：控制台、系统中心、服务器端、客户端等几个相互关联的子系统组成。每一个子系统均包括若干不同的模块,除承担各自的任务外，

还与其它子系统通讯，协同工作，共同完成对整个网络的病毒防护工作。本此项目系统主机层面的防病毒系统部署主要是在对外服务器区域和安全管理区域的重要服务器主机上，以及所有办公终端上部署防病毒产品。产品部署建议如下:

1、 在网络所有服务器主机和终端统一部署网络防病毒客户端;

2、 在安全管理区中部署一台网络杀毒服务器，安装网络版防病毒的服务管理端;

3、 在安全维护管理人员使用的终端设备上部署管理控制台程序，用于对防病毒服务器的状态和策略维护;

4、 病毒库升级工作由网络杀毒服务器自动联接互联网进行;

5、 机房服务器的防病毒系统可以自行连接互联网升级服务器进行升级。

3.6.3 主机安全管理

等级保护中对主机安全管理的技术要求

根据对 XXX 市智慧城市大数据中心应用系统保护等级达到**安全等级保护三级** S3A2G3 的基本要求，必须要符合以下技术要求:

1、 应能够对非授权设备私自联到内部网络的行为进行检查,准确定出位置，并对其进行有效阻断;

2、 应能够对内部网络用户私自联到外部网络的行为进行检查,准确定出位置，并对其进行有效阻断。

3、 应根据资产的重要程度对资产进行标识管理,根据资产的价值选择相应的管理措施;

4、 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储

等进行规范化管理。

5、 应实现设备的最小服务配置，并对配置文件进行定期离线备份；

6、 应保证所有与外部系统的连接均得到授权和批准；

7、 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；

8、 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

等级保护对主机安全管理的实现

实现以上对信息资产的收集、分类，实现系统的合理服务配置、限制非法的网络联接等，最直接的办法就是部署终端安全管理系统，该类系统具备资产收集和管理，终端服务进程管理、网络准入控制、检查网络非法外联等方面的功能。

根据上述情况，在 XXX 市智慧城市大数据中心网络中部署一套功能完备的终端安全管理系统，功能包括：

⑴ 终端安全管理功能

- 违规联网监控和 IP、MAC 绑定
- 移动存储设备监控审计
- 非正常终端阻止入网
- 软件安装行为限制

⑵ 终端资产管理功能

- 硬件资源管理
- 软件资源管理(包括安装软件和运行进程)
- 软件和进程黑、白名单监控功能
- 客户端任务分发（包括软件）分发
- IP 管理和设备入网管理功能

- 远程呼叫帮助维护平台

⑶ 补丁管理功能

- 客户端漏洞自动侦测
- 补丁自动下载安装

内网安全管理产品可以可以通过软件进行软阻断的方法对非正常主机和非授权主机联网进行阻断，防范非授权终端随意接入网络，从而防范内部涉密重要信息的泄露。内网安全管理及补丁分发产品系统能对非法接入计算机的行为进行报警，并能够自动阻断，如外来的笔记本电脑和新增设备的接入。

（1） 在网络所有服务器主机和终端统一部署内网安全管理系统客户端；

（2） 在安全管理区中部署一台网络安全监控服务器，安装系统的服务管理端；

（3） 在安全维护管理人员使用的终端设备上部署管理控制台程序，用于对管理服务器的状态和策略维护；

（4） 系统升级工作由管理服务器自动联接互联网进行。

3.6.4 应用安全设计

等级保护对应用安全防护的技术要求

根据对 XXX 市智慧城市大数据中心应用系统安全保护等级达到**安全等级保护三级** S3A2G3 的基本要求，信息系统对应用安全的防护，必须符合以下技术要求：

（1） 身份鉴别（S3）

本项要求包括：

- 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
- 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
- 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

（2） 访问控制（S3）

本项要求包括：

- 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
- 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；
- 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
- 应具有对重要信息资源设置敏感标记的功能；
- 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

（3） 安全审计（G3）

本项要求包括：

- 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
- 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
- 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
- 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

（4） 剩余信息保护（S3）

本项要求包括：

- 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

（5） 通信完整性（S3）

应采用密码技术保证通信过程中数据的完整性。

（6） 通信保密性（S3）

本项要求包括：

- 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
- 应对通信过程中的整个报文或会话过程进行加密。

（7） 抗抵赖（G3）

本项要求包括：

- 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
- 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

（8） 软件容错（A2）

本项要求包括：

- 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

（9） 资源控制（A2）

本项要求包括：

- 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
- 应能够对应用系统的最大并发会话连接数进行限制；
- 应能够对单个帐户的多重并发会话进行限制。

3.6.5 等级保护对网络应用安全的实现

根据 XXX 市智慧城市大数据中心应用系统为了达到等级保护三级要求，可以在互联网区域部署一台 SSLVPN，在安全管理区域部署安全运维管理平台进行日志收集整合，在核心交换机上部署负载均衡设备，以及在运维管理区域部署运维堡垒机等，具体实现措施如下：

(1) 可以通过 SSL 的访问管理方式实现传输过程中的保密和完整性要求;

(2) 通过在互联网区域部署一台 SSLVPN，提供给移动办公用户通过互联网或者其他区域不安全网络进行接入办公，并采用两重或者两重以上的身份认证机制，保障了数据完整性、保密性、安全性等多方面;

(3) 考虑到业务系统软件容错性方面，可以对其部署一台负载均衡设备，将业务系统在组成集群模式，当其中一个业务节点故障时，不会影响该业务业务正常运行，解决了业务系统可靠、稳定性等多方面问题;

(4) 在安全管理区域部署一台运维堡垒机，对所有内网安全设备、服务器进行运维时，所有操作行为能够有效审计溯源;

(5) 在核心交换机上旁路部署一台数据库审计设备，对所有数据库操作的行为进行安全审计，保障数据库操作日志不可删除性。

3.6.6 数据安全及备份恢复设计

等级保护对数据安全及备份恢复的技术要求

根据对 XXX 市智慧城市大数据中心应用系统安全保护等级达到安全等级保护三级 S3A2G3 的基本要求，信息系统数据安全及备份恢复，必须符合以下技术要求:

(1) 数据完整性（S3)

本项要求包括:

- 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施;
- 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程

中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

（2） 数据保密性（S3）

本项要求包括：

- 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；
- 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

（3） 备份和恢复（A2）

本项要求包括：

- 应能够对重要信息进行备份和恢复；
- 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

3.6.7 等级保护对数据安全及备份恢复的技术实现

根据 XXX 市智慧城市大数据中心应用系统为了达到等级保护三级要求，对于 XXX 市智慧城市大数据中心应用系统数据安全及备份恢复实现方式具体如下：

（1） 构建 PKI/CA 认证体系，对重要应用系统采用 PKI/CA 认证方式进行授权认证访问，保障了数据安全的抗抵赖性、完整性、保密性；

（2） 通过 SSL 加密访问管理方式实现传输过程中的保密和完整性要求；

（3） 对于存储的保密性和完整性要求可以通过加密存储介质来进行存储，并建立异地灾备中心，采用实时数据同步系统，自动进行数据

库增量备份，保障其完整性；

(4) 对系统或者数据库可以采用主备或者集群方式进行，并结合负载均衡设备更好地解决单点故障问题。

3.6.8 系统运维管理安全设计

等级保护对系统运维管理安全的技术要求

根据对 XXX 市智慧城市大数据中心应用系统安全保护等级达到安全等级保护三级 S3A2G3 的基本要求，系统运维管理安全必须符合以下技术要求：

(1) 网络安全管理方面

本项要求包括：

- 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理；
- 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补
- 应定期对运行日志和审计数据进行分析，以便及时发现异常行为

(2) 监控管理和安全管理中心方面

本项要求包括：

- 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理

等级保护对系统运维管理安全的技术实现

根据 XXX 市智慧城市大数据中心的网络情况现状分析，为了达到等级保护三级要求，对于 XXX 市智慧城市大数据中心应用系统的系统运维管理安全实现

方式具体如下：

(1) 通过部署安全运维管理中心，对全网应用系统、安全设备等进行日志收集整合，实时监测全网安全情况，并通过短信、邮件等方式自动进行报警反馈等功能；

(2) 通过部署终端安全管理系统，可以对终端、服务器等设备进行安全补丁统一管理修复，及时解决系统安全问题；

(3) 通过部署漏洞扫描系统，及时对全网应用系统、安全设备等进行漏洞扫描，并自动生成报表进行反馈，及时修复对应安全漏洞。

四、 配置清单

XXX市云计算平台					
序号	项目	类型	型号	参数	数量
1	云服务器资源池	金牌资源池	TS860	8颗12核心Intel E7-8857 v2 3.0GHZ处理器，256GB 内存，3块10000转 2.5" 300G SAS硬盘，配置8通道高性能RAID卡，1GB高速缓存待电池保护，支持raid0,1,5,4个千兆网卡，支持虚拟化加速、网络捆绑等功能,独立光纤万兆网卡四口配置SFP+光模块，配置2张单口8G HBA卡，1个8G SFP光模块，2+1电源冗余，支持远程安装操作系统、远程开关机、远程控制等，配置导轨附件，含现场安装培训及3年售后服务。	11
2		银牌资源池	NF8460M3	4颗12核心Intel E7-4850 v2 2.3GHZ处理器，128GB内存，3块10000转 2.5" 300G SAS硬盘，配置8通道高性能RAID卡，1GB高速缓存待电池保护，支持raid0,1,5,4个千兆网卡，支持虚拟化加速、网络捆绑等功能,独立光纤万兆网卡四口配置SFP+光模块，配置2张单口8G HBA卡，1个8G SFP光模块，2+1电源冗余，支持远程安装操作系统、远程开关机、远程控制等，配置导轨附件，含现场安装培训及3年售后服务。	34
3		铜牌资源池	NF5270M4	2颗10核心Intel E5-2650 v3 2.3GHZ处理器，64GB内存，3块10000转 2.5" 300G SAS硬盘，配置8通道高性能RAID卡，1GB高速缓存待电池保护，支持raid0,1,5,4个千兆网卡，支持虚拟化加速、网络捆绑等功能,独立光纤万兆网卡2口配置SFP+光模块，配置2张单口8G HBA卡，1个8G SFP光模块，2+1电源冗余，支持远程安装操作系统、远程开关机、远程控制等，配置导轨附件，含现场安装培训及3年售后服务。	6

4	存储资源池	SAN+NAS 统一存储	AS8000-M2	SAN+NAS 统一存储，每个存储节点并行架构双控制器 Active/Active，本次配置存储组存在 4 个并行架构控制器，高速缓存 256GB，配置 16 个 8Gbps 的光纤 FC 接口，配置 48 块 800GB SSD 硬盘，配置 96 块 900GB 10K 转速 SAS 硬盘，配置 96 块 4TB NL SAS 7.2K 硬盘，配置自动层软件，配置精简配置软件，配置数据快照软件，配置原远程镜像软件。	1
5	FC SAN 资源池	FC 光纤交换机	Brocade 5300	Brocade 5300 是一款 8 Gbps 光纤通道交换机，可提供卓越的性能和端口密度，适用于要求最为苛刻的 SAN 环境，2U 的机架式外形，激活 80 个光纤通道端口， 配置 80 个 8GB SFP 模块，640 Gb / 秒带宽，3 年服务。	2
6	备份设备	备份一体机	DP1000-M1	备份存储一体机；配 2 个万兆备份接口,支持万兆备份接口；配 16GB 缓存，最大支持不小于 32GB，配 100TB 备份裸容量，后续容量可无缝扩展至 368TB，提供开通所有数据备份许可，不限应用端数量，提供 ERP、数据重删以及远程备份等高级备份功能；多个备份任务可以并行同时执行；备份软件对所有已备份数据和磁带介质的管理应简单高效，备份数据列表可以快速查找和浏览；应具备详尽的历史日志记录、查询、管理和报告功能；能提供容灾备份/恢复功能；支持 Windows、Linux、unix 等多种操作系统；支持 Oracle、SQL Server、DB2 等各类系统平台数据库备份,ERP、exchange 等应用文件备份，操作系统快速备份等含现；支持异构厂商服务器平台，支持异构硬件备份介质；场安装培训以及 3 年售后服务	2
7	云平台软件	虚拟化软件	InCloud Sphere	浪潮 InCloud Sphere V4.0 iNode 企业版 236 颗 CPU 授权	1
8		虚拟化管理软件	iCenter	InCloud Sphere V4.0 iCenter 企业版一套	1
9		云平台管理软件	云海 OS V3.2	云海 OS 云平台高级版软件授权，每 25 个 VM1 个授权，即 1 个授权可使云平台管理 25 个 VM。高级版内容包括：系统管理；系统安全增强；云资源管理；业务流程管理；计量计费；应用监控与智能分析等。	70
10	数据中心网络	云平台核心交换机 2 台	RG-N18010 组合配置包 01	N18010 组合配置包 01，含：（主机）1×RG-N18010（引擎）2×M18010-CM（网板）2×M18010-FE-D I（电源）4×RG-PA1600I	2
11			M18010-FE-D I	N18010 交换网板 I（配合 ED/DB 线卡使用）	4
12			M18000-24QXS-DB	24 端口 40G 以太网光口(QSFP+,MPO)	4
13			M18000-48XS-DB	48 端口万兆以太网光口(SFP+,LC)	2

14			M18000-24GT20SFP4XS-ED	24 端口千兆以太网电接口板(RJ45)+20 端口千兆以太网光口(SFP,LC)+4 端口万兆以太网光口(SFP+,LC)	2
15		云平台服务器接入交换机 20 套	RG-S6220-48XS4QXS	固化 48 个 10G SFP+端口,4 个 40G QSFP+端口,序号 1~8 端口为统一通信接口(支持 FC/FCoE/10GE 三种使用模式,FC 模式支持 8/4/2Gbps 自适应),不含电源和风扇,对应风扇型号为 M6220-FAN-F	20
16			M6220-FAN-F	主机风扇（前后风道散热），最少配置 3 个风扇，最多配置 4 个风扇，可实现 3+1 冗余	80
17			RG-M6220-AC460E-F	主机电源（前后风道散热），最少配置 1 个电源，最多配置 2 个电源，可实现 1+1 冗余	40
18		局域网区核心交换机 2 台	RG-S8610 组合配置包 01	RG-S8610 组合配置包 01，含：（主机）1×S8610-Chassis（引擎），1×M8610-CM III，（电源）2×RG-PA1200E	2
19			M8600-16XS-DA	16 端口 SFP+的万兆线卡	4
20			M8600-24SFP/12GT-EC	24 个 SFP 千兆通用接口+12 个复用 10/100/1000M 自适应电口 EC 线卡	2
21		局域网区域接入交换机 5 台	RG-S2928G-E	24 口 10/100/1000M 自适应电口交换机，4 个 SFP 光口	5
22		云平台测试区接入交换机 2 套	RG-S6220-48XS4QXS	固化 48 个 10G SFP+端口,4 个 40G QSFP+端口,序号 1~8 端口为统一通信接口(支持 FC/FCoE/10GE 三种使用模式,FC 模式支持 8/4/2Gbps 自适应),不含电源和风扇,对应风扇型号为 M6220-FAN-F	2
23			M6220-FAN-F	主机风扇（前后风道散热），最少配置 3 个风扇，最多配置 4 个风扇，可实现 3+1 冗余	8
24			RG-M6220-AC460E-F	主机电源（前后风道散热），最少配置 1 个电源，最多配置 2 个电源，可实现 1+1 冗余	4
25		广域网路由器 2 台	RG-RSR7708	RSR7708 主机箱（双路由引擎插槽，4 个业务载板插槽，8 个业务子卡插槽，带风扇盘、防尘网），路由引擎、业务载板及子卡、电源需要另外购买，支持热拔插	2
26			RSR7708-SRCMI	RSR7708 路由引擎，固化 1 个 10M/100M/1000M 口，2 个 USB 2.0 口，1 个 SD 卡插槽，1 个 Console，1 个 AUX，2G 内存，512M FLASH	4
27			RG-PA300I	交流电源模块（可以冗余，300W，配 10A 电源线）	6
28			RSR77-SIP1	FNM 业务处理卡载板，512M 内存，2 个 FNM 业务处理卡插槽	2
29			FNM-2XS	2 端口万兆以太口接口模块，需另配 SFP+光模块	4
30			DFNM-32GT/16SFP	32 端口千兆电口+16 端口千兆光口以太网接口模块，若使用光口则需另配 SFP 光模块	2

31	数据中心安全	一体化安全网关	天清汉马 USG-14600-GP-C	标准 2U 设备,双冗余电源；标配 5 千兆电口，4 个 SFP 插槽，2 个万兆 SFP 插槽； 包含三年 AV 病毒库升级、三年上网行为特征库升级、三年产品基本服务	4
32		安全接入网关	天清汉马 SAG-6000-2000N-QD	标准 1U 机箱，单电源；网络接口：8 个 10/100/1000M Base-TX；4 个 SFP 插口；包含 500 个 SSLVPN 并发用户授权、三年产品基本服务	2
33		Web 应用安全网关	天清汉马 WAF6000-A	2U 上架设备，1 个 HA 口，1 个 RJ-45 Console 口，1 个 10/100/1000 Base-T 带外管理口，4 个网络接口板扩展槽位，可选配天清 WAG-NIM-L 通用接口板，默认含 3 个接口（含 1 个 HA 接口）永久使用授权），2 个 USB 口，双电源；含一个 WAF-NIM-L-2SFP+接口板（不含光收发模块）、HTTPS 应用防护模块使用授权、三年 Web 应用防护特征库升级授权、三年产品基本维保服务	2
34		入侵防御系统	天清汉马 NGIPS5000-A	2U 上架设备，1 个 RJ-45 Console 口，2 个 10/100/1000 Base-T 带外管理口，4 个网络接口板扩展槽位，可选配天清 NGIPS-G 系列专用接口板，2 个 USB 口，双电源，含 1 个 NGIPS-G-BYPASS-2SFP+扩展模块（自带 2 个多模光纤收发模块）、三年入侵特征库升级、高级威胁检测模块以及三年升级服务、三年产品基本服务	2
35		安全管理平台	泰合 TSOC-USMv3.0.20.2	包含中心系统软件一套、增加 50 个管理节点、资产建模模块、基础监控模块、漏扫调度管理模块、配置安全核查模块	1
36		终端安全 管理系统	天珣内网安全风险管理与审计系统企业版 V6.6.9.6	包含系统介质包、企业版控制台管理授权、客户端授权许可 500 个、3 年产品升级服务	1
37		漏洞扫描系统	天镜脆弱性扫描与管理系统 CSNS-H3	包括 2U 上架设备，标配 1 个 10/100/1000M 管理口（可做扫描口）、1 个 100/1000M 扫描电口（扫描口可扩展，最多可新增 4 个电口和 4 个光口（扩展光口需单独采购 SFP 模块））。天镜 600 非固定 IP 授权，包含三年硬件维保、系统扫描漏洞库三年升级服务、web 扫描模块授权、三年 web 扫描特征库升级授权	1
38		运维堡垒机	天玥网络安全审计系统 OSM-5200	2U 机架式软硬一体设备,专用硬件平台和安全操作系统，6 个千兆电口，1 个 console 管理口，硬盘容量 3TB，内置 raid，双电源；包含一个 OSM-5X-4SFP 扩展板（不含光模块）、一个 500 点被管资源授权、三年产品基本维保服务	1

39		数据库审计	天玥网络安全审计系统 CA6500-ER+CA6500-SR	包含一台 6500 审计引擎（千兆引擎、2U 上架专用设备、2 个千兆电口监听口、1 个千兆管理口、双电源、支持一个千兆/万兆扩展板）、一台 6500 审计数据中心（千百兆引擎的审计数据中心、2U 上架专用设备、1 个千兆电口管理口、1 个千兆电口数据口、数据存储量 3*2T、支持 RAID5、双电源）、两个 CA-Slot-2XFP 扩展板（不含光收发模块）、1 个 50 个被审计 DB 的授权、两个个 CA 监听端口授权、三年产品基本维保服务	1
40		入侵检测管理系统	天阗 IDS 入侵检测与管理系统 NT12000-LT-B	2U 上架设备，1 个 RJ-45 Console 口，2 个 10/100/1000 Base-T 带外管理口，4 个监听口扩展槽位，可选配 NT12000 系列千兆、万兆扩展板卡，2 个 USB 口，冗余电源，专用扩展板 4*SFP+（包含 4 个 SFP+多模光收发模块）、WEB 服务器攻击检测模块、4 个监听模块、3 年入侵特征库升级、3 年基本产品维保服务	1
41		负载均衡系统	天清 ADC-4004 应用交付控制器	性能 4Gbps，最大可扩展到 10Gbps。提供服务器负载均衡、多链路负载均衡、链路拥塞控制，智能 DNS，动态就近性探测，TCP 单边加速等功能，四层防火墙功能。 1U 上架设备,单电源,1 个 10/100/1000M 管理接口,5 个 10/100/1000M 自适应电口,1 个 ADC-NIM-L 通用扩展插槽，含嵌入式软件；包含一个 ADC-NIM-L-2SFP+扩展接口板（不包含光收发模块）、七层防火墙授权、三年基本维保服务	2
42		实时数据 同步系统	合众 RDS（软件版）	数据自动同步备份	1
43		病毒防御系统	网络病毒防御系统	进行全网终端以及服务器病毒防护（按照服务器端＋终端一共 500 个点预估）	1
44		安全运维服务	启明星	两人三年驻场服务	6
45		等保三级 安全测评	等保三级安全测评	信息系统梳理、调研	1
46		等保三级安全测评	等保三级安全测评	信息系统定级、备案	1
47		等保三级安全测评	等保三级安全测评	信息安全等级保护等保现场测评	1
48		等保三级安全测评	等保三级安全测评	出具信息系统等级保护测评报告	1