# 哈尔滨市航空服务中等专业学校
# 云数据中心建设方案

# 第一部分 云数据中心总体方案

## 一、指导思想

以习近平新时代中国特色社会主义思想为指导，深入贯彻党的十九大和十九届三中、四中、五中全会精神，全面贯彻落实全国教育大会精神，深化教育领域“放管服”改革，以数据为驱动力，利用新一代信息技术提升教育管理数字化、网络化、智能化水平，推动教育决策由经验驱动向数据驱动转变、教育管理由单向管理向协同治理转变。以建设为基础、应用为支柱，以促进学校管理、服务教师、服务学生及学生家长为核心，以建设数字化、网络化、智慧化校园环境为目标，促进优质管理、优质教育教学资源共享、家校联系，全面提升学校教育信息化、现代化水平。

## 二、建设目标

利用云计算技术打造学校大数据分析、高性能应用等学校科研基础平台。

云数据资源中心建设后，将包括校园云计算虚拟化中心、大数据分析和高性能计算中心，并为此三个中心提供统一管理平台。通过云数据中心的建设，物理资源将被组织起来统一调配和供应，提供给学校各部门、教师及学生使用。并且通过云数据中心为学校提供大数据分析和高性能计算服务。通过资源集中化，资源的共享得以实现。从而解决数据中心当前面临的问题，更有效的推动信息化的发展。

基于云计算的大数据和高性能中心建设目标主要有以下几个方面：

1.资源集约化。通过虚拟化方式，为各部门和师生提供基础计算服务和数据存储。

2.数据一体化。方便数据共享，为大规模数据整合和交换提供可能。

3.管理服务化。利用云计算方式，实现基础软硬件资源的统一管理、按需分配、综合利用，降低各部门系统建设成本和日常运行维护费用。

建设完成后的高校云计算平台实现以下功能：

1.建设服务器虚拟化中心；为学校各大业务平台提供IAAS服务，以虚拟服务器的方式为校园各大业务平台提供业务支撑服务；

2.建设大数据分析；为前沿的大数据分析和研究提供服务，为部分在校学生课题提供服务；

3.建设校园高性能计算中心；为学校一些需要进行高性能计算的部门提供高性能计算基础平台，为业务部门高性能计算需求提供服务；

4.建设云计算中心统一管理平台；为校园云计算中心中的业务云平台、大数据分析系统、高性能计算中心提供统一的管理平台，为不同管理用户和业务用户提供统一入口；

5.通过建设云计算平台，学校实现对资源的大集中统一管理并提升整体计算能力；通过虚拟化技术提高资源利用率，避免重复建设，节约整体成本。

## 三、设计原则

智慧校园建设必须遵循“统一规划、分步实施”和“以需求为导向，以应用促发展”的原则。

1.成熟性与发展性的统一的原则。

应首先采用符合当前计算机及应用系统发展趋势的主流技术。既要保证当前系统的高可靠性，又能适应未来技术的发展，满足多业务发展的要求。要本着“有用、适用和好用”的原则，不片面追求软硬件设施的先进性，应强调整个系统的可连接性和整体布局、应用的合理性。

2.先进性与实用性的统一。

技术必须具有先进性和前瞻性和实用的原则，在满足性能价格比的前提下，坚持选用符合标准的，先进成熟的产品和开发平台。

3.独立性与开放性的统一。

各系统相互独立又相互关联，因此在规划和设计过程中需要考虑本系统的独立性，以及多系统间的融合和关联。

4.可配置性。

由于整个系统建设涉及的部门比较多，业务种类比较复杂，因此系统的灵活配置性就显得非常重要，系统的可配置性应包括部门配置、人员角色配置、公文样式配置、处理流程配置等。

5.标准化。

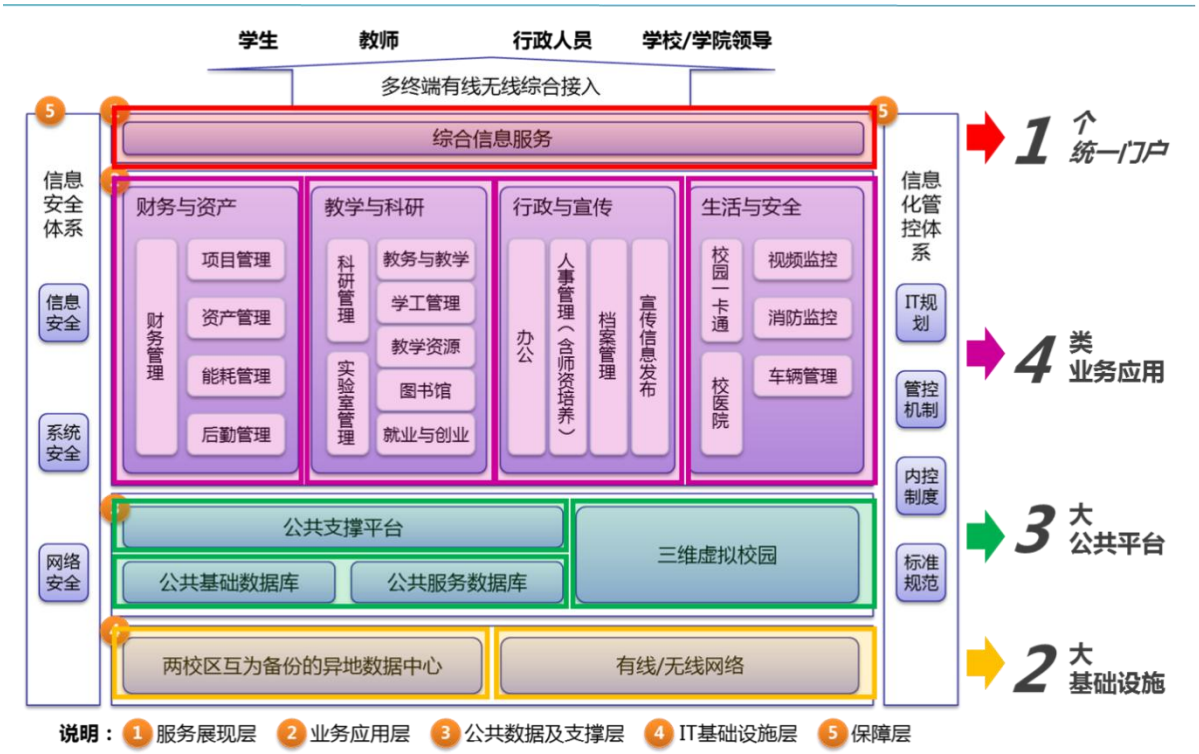
现有信息技术的发展越来越快，为了使该系统在未来运行过程中其技术能和整个信息技术的发展同步，系统应具有备灵活适应性和良好的可扩展性，系统的结构设计和产品选

型要坚持标准化，首先采用国家标准和国际标准，其次采用广为流传的实用化工业标准。

6. 可靠性、安全性、保密性。

智慧校园建设涉及面广，设计上要充分考虑其大量硬件设备、软件系统和数据信息资源的实时服务特点，要保证网络、系统、数据的安全，保证系统运行的可靠，防止单点故障，对涉密信息应充分保证其安全。对安全管理要充分考虑安全、成本、效率三者的权重，并求得适度的平衡。对整个系统要有周密的系统备份方案设计。对系统主要的信息实行自动备份，以保证系统的异常情况的补救，并设有系统自动恢复机制。采取必要措施防止数据丢失，保证数据的一致性，保证系统运行过程中的高可靠性。

## 四、智慧校园整体架构




智慧校园架构分为五层，分别是基础设施层、公共平台

层、业务应用层、统一门户层、业务安全保障层。

基础设施层：包括三个层次的基础设施架构，包括云服务、云数据中心、云校园网络。

公共平台层：保留公共支撑平台以及一些公共数据库、地理位置信息数据库等。

业务应用层：包括财务资产、教学科研、行政服务、生活服务等四大模块。

统一门户层：综合信息服务通道。

业务安全保障：包括网络安全、数据中心安全等，部署校园信息安全防御体系。

## 第二部分 云数据中心详细设计

### 一、总体架构设计

#### （一）逻辑架构设计

云数据中心总体架构设计遵循面向业务需求的设计思路，基于模块化的设计方法，实现数据中心 IT 基础架构模块与业务模块松耦合，保证数据中心业务动态扩展和新业务快速上线。

使用特定规格产品设计，包括硬件、软件和应用规格化来提供简单可靠、易于部署和管理、便于扩展和升级的 IT 基础架构，满足学校数据中心建设以及数据中心的可视化统一管控的需求。

学校云数据中心建设的逻辑架构参考如下：


整体架构自底向上为云机房基础设施层、云计算基础架构层（基础资源层和灾备层）、业务应用层、服务对象层，以及数据中心的安全保障和数据中心统一管理。

1. 云机房基础设施层：基于业务需求的模块化数据中心的设计与实现。

2. 云计算基础架构层：主要涉及基础资源层与容灾备份层。

3. 基础资源层：也可叫云服务层，包括服务器设备、存储设备、网络设备、安全设备、虚拟化软件，以及通过虚拟化平台构建的虚拟化资源池，还有物理资源池，可以通过智能资源调度与管理平台对虚拟资源池与物理资源池统一管理，并对上层应用系统提供 IT 服务，云服务层是校园信息化的基础架构。云服务层还包括高性能计算解决方案、大数据平台方案等。

计算：本解决方案所提供的计算系统的设备为服务器，服务器要配合数据中的的云操作系统，可以为用户提供高计

算密度、高资源利用率、以业务为导向的易管理的计算系统。根据实际业务需求，结合安全和管理需求，除数据库服务器和管理服务器不虚拟化外，其他服务器将充分采用虚拟化技术。

存储:存储与计算分离，存储采用 FC SAN 连接主存储阵列。通过虚拟化集中部署，动态分配和调用资源，实现计算和存储资源的高效管理。同时部署大数据存储服务，高性能计算服务。

虚拟化平台：统一虚拟化平台通过对服务器物理资源的抽象，将 CPU、内存、I/O 等服务器物理资源转化为一组统一管理、可灵活调度、动态分配的逻辑资源，并基于这些逻辑资源在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。

虚拟资源池：采用虚拟化技术实现 IT 基础设施的资源池化，为上层业务提供 IT 资源弹性供给，更好地实现 IT 资源共享，提高利用率，快速响应业务需求。

物理资源池：包括数据库物理机部署以及物理机集群等。

智能资源调度与管理：同时提供物理资源和虚拟资源的统一监控管理，进而提供全生命周期资源服务。即对计算、存储、网络资源的池化管理构建虚拟数据中心。

4.容灾备份层：提供容灾和备份的解决方案。考虑业务的连续性，按照容灾等级可以提供应用容灾和数据容灾，在本项目中主要考虑核心业务如管理平台与资源平台的数据的安全性与业务的连续性。

构建本地备份系统，实现基础数据库系统备份与虚拟机系统备份，实现数据库数据与业务运行环境保护。

建设双活灾备系统，首先实现数据库存储级数据双活容灾，再实现业务级双活容灾。

5.业务应用层：包括学校的核心业务，如一卡通系统、教务系统、教学系统、科研系统、办公系统、资产系统等，以及包括支撑校内主要业务、共享数据和交互数据等内容的核心数据管理，是学校各机构整体信息化的基础数据环境。各种业务数据来源包括由学校各部门现有的各种业务处理应用系统（例如教务、办公、一卡通等应用系统）等提供的业务数据。

6.服务对象层：涉及到业务应用层的使用者，可以通过统一门户平台获取到相关的服务。

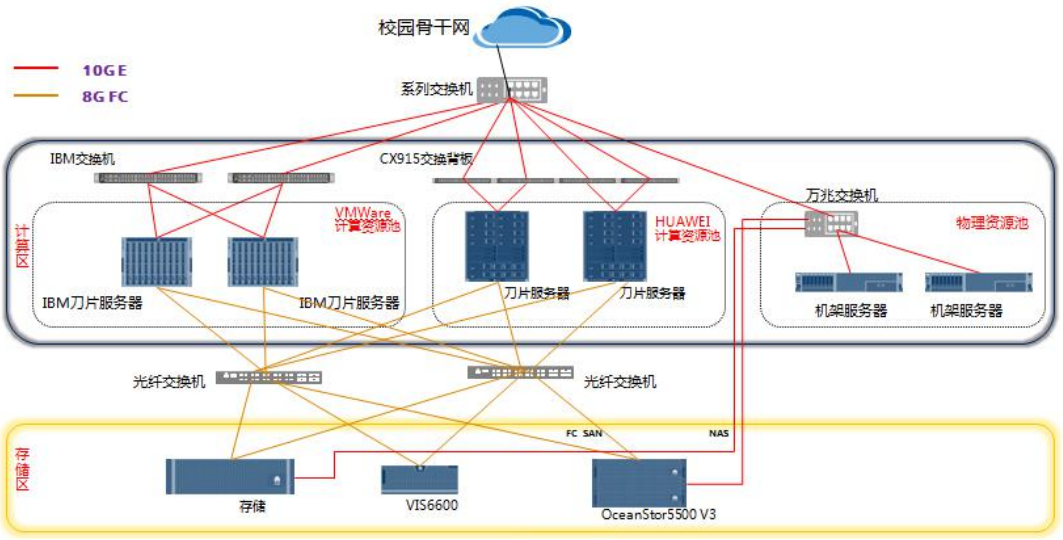
7.数据中心安全保障：一体化安全保障系统从物理设施安全、网络安全、主机安全、虚拟化安全、数据安全、应用安全、用户接入安全、安全管理等多层次为政务系统运行提供全方位安全保障。

8.数据中心统一运维管理：云数据中心运维管理采用开放的管理架构和模块化的设计思路，根据云数据中心管理需求配置运维管理模块。主要管理模块包括服务管理、统一管理门户、服务流程管理、综合监控管理以及云计算平台管理。为了保证方案的开放性和可扩张性，运维管理架构采用业界成熟管理产品与管理产品相结合。

**（二）物理架构设计**

云数据中心建设内容包含网络、服务器、存储等基础设备的部署与管理，核心业务如校园管理公共服务平台、数字图书馆、邮件系统等业务的云平台部署，平安校园监控、视频教学的物理部署，桌面云办公平台部署。

云数据中心物理架构示意图如下：




本项目中，将数据中心的物理部署架构分成了三区，即网络区、服务器区、存储区：

1. 网络区：即数据中心网络架构层，采用扁平化二层网络架构（核心层、接入层），使用网络虚拟化技术，核心交换机承担着核心层和汇聚层的双重任务。

2. 服务器区：提供计算能力的服务器设备，服务器要配合虚拟化操作系统，为用户提供高计算密度、高资源利用率、以业务为导向的易管理的计算系统。根据实际业务需求，结合安全和管理需求，除一些特殊应用不虚拟化外，其他服务器将充分采用虚拟化技术。

服务器区主要包括核心业务的云计算资源池，非结构化数据业务的物理集群的物理资源池。

云计算资源池：通过统一虚拟化平台对服务器物理资源的抽象，将CPU、内存、I/O等服务器物理资源转化为一组统一管理、可灵活调度、动态分配的逻辑资源，并基于这些逻辑资源在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境，虚拟资源池是通过这些逻辑资源构建的。在本项目中，针对邮件系统、办公系统、一卡通系统、教务系统、数字图书馆等教育相关的业务系统。通过虚拟化技术提高业务的敏捷性，使得教育应用在资源利用上弹性可伸缩。通过将业务与具体物理机解耦合，实现业务在计算资源池内灵活迁移，不受具体物理机故障的影响。云计算平台业务通常采用刀片服务器。

物理资源池：对于非结构化数据的多媒体应用业务，如校园安全的视频监控业务、远程视频教学业务对于业务处理的实时性要求很高，业务数据的安全性要求也很高，建议采用物理机集群方式部署可以更好地保障业务高效性。对CPU和内存要求高的关键应用如校园监控，实时远程教学等可以选择4-8路CPU的机架服务器。

3.存储区：存储与计算分离，虚拟化平台业务存储采用FC SAN连接主存储阵列。通过虚拟化集中部署，动态分配和调用资源，实现计算和存储资源的高效管理。同时对于核心业务数据通过镜像卷技术实现本地存储高可用，以及后续的双数据中心容灾的平滑演进。对于非结构化数据的多媒体应

用业务，存储采用 NAS 存储提供高带宽、高并发的文件共享服务。

## 二、数据中心云平台设计

### （一）数据中心云平台架构

云平台总体架构设计遵循面向业务需求的设计思路，基于模块化的设计方法，实现数据中心 IT 基础架构模块与业务模块松耦合，保证数据中心业务动态扩展和新业务快速上线。云数据中心是校园业务部署的主要支撑平台，需要整合分散在各处的服务器、存储与网络设备资源，通过云操作系统的虚拟化平台实现服务器虚拟化、存储虚拟化、网络虚拟化，构建全校共享的硬件资源池，通过云操作系统的智能资源调度管理平台实行资源的分配、调度与管理，快速响应教育信息化的业务需求。

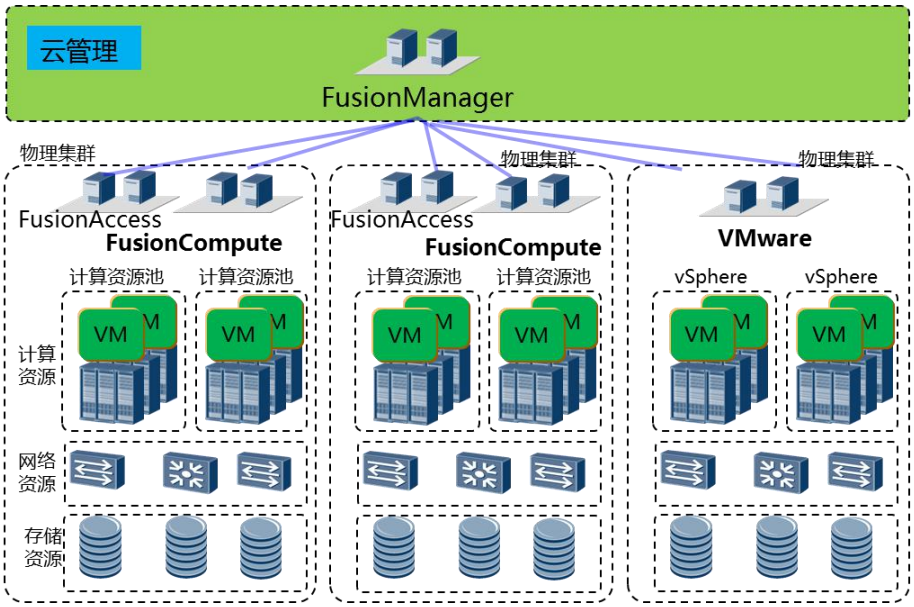
云数据中心架构分为三层，分别是基础设施层、虚拟化资源层、云服务统一管理层。

基础设施层由服务器、网络设备、备份设备、安全设备和存储设备组成。

虚拟化资源层用于帮助客户收编现有的资源池，实现资源的统一管理和共享。并且提供 VDC 虚拟数据中心的逻辑隔离的技术，将物理资源池化后，按组织、业务需要灵活分配，构建的一个逻辑的数据中心，为用户提供最贴心的资源共享和分配方案。

云平台支持服务器、存储的平滑扩容。服务器、存储设备均可根据业务根据需求，在线平滑增加服务器、服务器虚拟集群，在线扩展磁盘、磁盘框、控制框。

### （二）异构云计算资源池统一管理




## 三、云平台服务设计

面对目前学校一个云平台可能存在多种虚拟化平台的现状。建设统一融合资源池，实现多资源池统一管理，实现真正的管理统一。

将所有设备，包括安全、网络、虚拟化资源，形成一个校园云平台的集合。

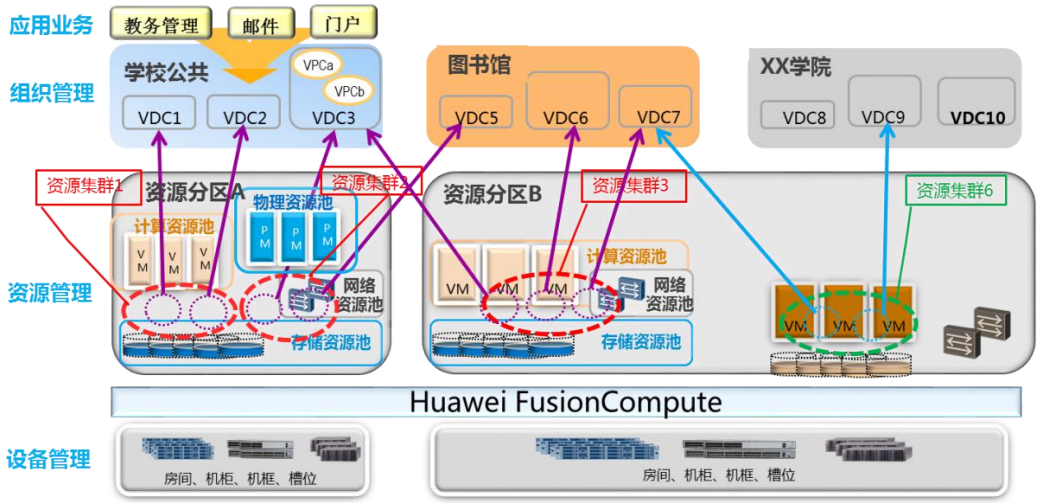
对异构虚拟化平台进行管理对接。按业务对物理资源和虚拟资源进行统一的管理和 SLA 设定，基于 SLA 实现校园云平台资源的策略发放和调度，自动化配置。以 VDC 的方式实现分权分域管理，降低管理成本。此外，通过网络打通实现跨地域异构虚拟化资源池自动化管理。

针对学校不同部门独立管理的诉求，通过 VDC 实现资源的相互隔离，互不干扰。

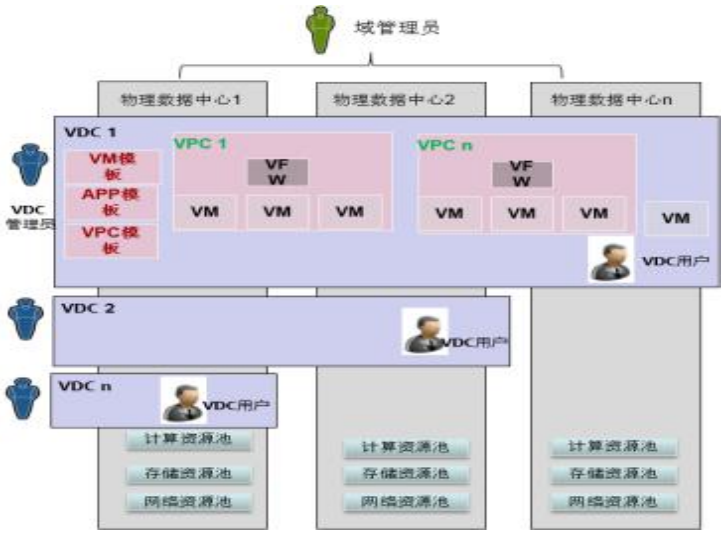
按照应用业务属性和安全分级进行资源域划分设计。一个完整 VDC 包括配额、用户、服务目录、网络、资源、模板。

通过 VPC 满足不同学校或部门的应用安全隔离。学校部门可在资源池中自行创建云主机、云存储、虚拟网络、负载均衡、弹性 IP 等基础设施服务。

### （一）虚拟校园云平台（VDC）服务




将学校物理校园云平台根据各业务部门需求灵活划分成 VDC，每个 VDC 可以独立提供的服务完全和物理校园云平台一样服务，每个 VDC 都有自己的管理员、服务目录等，VDC 管理员可以直接管理、审批 VDC 内用户的服务申请。VDC 之间的资源和网络相对隔离，同时可以通过 VDC 跨物理校园云平台，实现多个物理校园云平台资源的统一发放和调度。




将校园云平台之中的物理资源进行“池化”，可以根据各个部门不同的诉求灵活划分和分配物理资源，同时提供对应的服务，并让各个部门独立管理以及使用本 VDC 的资源，将整个校园云平台的超级管理员的工作进行分摊以及管理上分权，降低超级管理员的管理成本,更灵活的满足不同部门、用户的要求。

系统管理员作为所有资源的管理员可以将学校整个校园云平台的计算、存储、网络资源划分到各个 VDC，分配给各个部门。

VDC 管理员作为 VDC 的所有者，可以在 VDC 里定义模板、定义 VPC，发放 VM 等操作，是最终的使用校园云平台资源的组织的管理员。

最终用户作为某个 VDC 的业务最终使用者，可以通过自主平台或者线下申请 VDC 内的资源。

通过 VDC 管理，让学校各业务部门拥有自己独享的校园云平台。

**（二）虚拟私有云（VPC）服务**

VPC（Virtual Private Cloud）提供隔离的虚拟机和网络环境，满足不同部门网络隔离要求，可以提供直联网络、路由网络和内部网络多种组网模式。

每个 VPC 可以提供独立的虚拟防火墙、弹性 IP、安全组、VPN、NAT 网关等业务。此外，VPC 还可以提供各类资源的计次或流量统计信息，可作为计费系统的输入。

VPC 管理，满足所有应用的网络和安全需求。

VPC 网络应用场景：

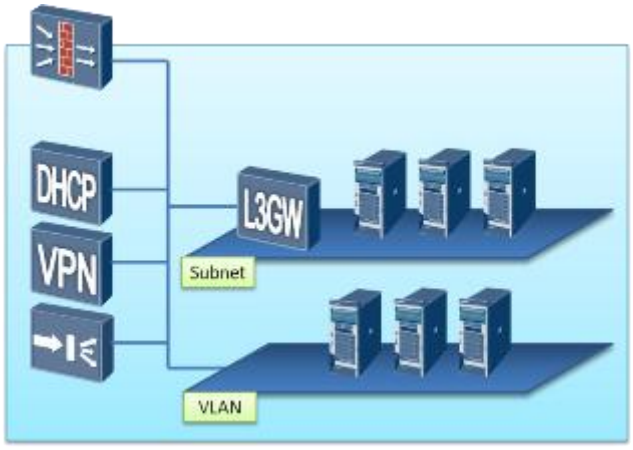

为满足不同部门的应用安全隔离的需求，学校云校园云平台公共服务平台为各部门提供虚拟私有云（以下简称 VPC）服务。

学校云校园云平台公共服务平台为每个要进行应用部署的各部门分配一个独立的 VPC。VPC 能够为各部门提供安全、隔离的网络环境，实现各部门间应用的隔离，及外部网络访问的安全控制。

在各部门的 VPC 中，拥有独立的网络边界：虚拟防火墙、VPN、NAT；

能够部署独立的内部网络能力：多平面，地址管理，DHCP，安全组，负载均衡器等。各部门可以在 VPC 中定义与传统网络无差别的虚拟网络，以满足业务部署要求。

VPC 内部资源示意图：

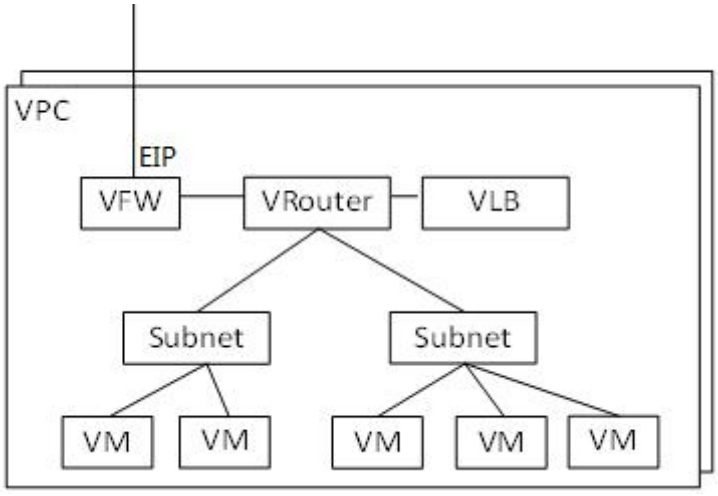



1.应用部署使用

各部门需要部署应用时，需要将虚拟云主机挂在自己的虚拟机内部，即可实现与虚拟机网络的互联，及与其他 VPC 云主机的隔离。

各部门在 VPC 内部可以通过划分子网的方式，实现不同应用间的隔离；通过负载均衡服务，实现大访问量业务的虚拟机负载均衡；通过虚拟防火墙实现对 VPC 外部的隔离。可以通过弹性 IP 与内部虚拟机或负载均衡的内部地址映射实现互联网用户对于应用的访问。

VPC 内应用部署逻辑图：




2.与各部门局域网对接

VPC 是在学校云校园云平台的云环境中构建的具有自己私有网络的云服务，能够与各部门的网络互通。在 VPC 中，各部门具有完全独立的 IP 地址空间设置，以及与其他各部门 VPC 的虚拟机的完全网络隔离。

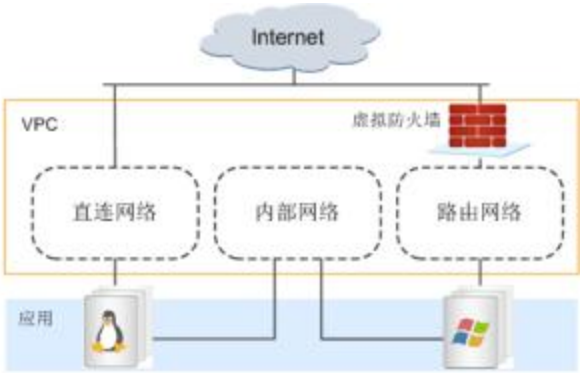
VPC 提供三种网络，协助学校各部门部署业务应用及对外服务。

直连网络：直连网络与外部网络相连，其自身不包含任何网络资源，在直连网络中创建虚拟机或应用时实际使用的是外部网络中的资源。外部网络可以是各部门现有网络或者公网。当外部网络为各部门现有网络时，直连网络与各部门现有网络对接，虚拟机可分配到各部门现有网络得 IP 地址资源。当外部网络为公网时，其直连网络中的虚拟机具有直接访问公网的能力。

内部网络：独享一个网络资源，该网络与其他网络安全隔离。由于内部网络和其他的网络是隔离的，因此内部网络中可以部署对安全性要求较高的业务，例如，可将数据库所在服务器部署在内部网络中，以保证数据安全。

路由网络：路由网络具有灵活的互通能力和多种业务功能，基于虚拟防火墙的路由网络能够与 VPC 中的其他路由网络互通，或者绑定弹性 IP 与公网进行通信。除了弹性 IP，路由网络还能提供 ACL、DNAT 和 VPN 业务，以满足业务部署要求。在创建路由网络前，需要先为 VPC 申请了虚拟防火墙。

VPC 及其网络的逻辑结构下图所示：




**（三）虚拟主机服务**

智慧校园云平台可为各部门提供虚拟主机租用服务，各部门管理员可以在公共平台上对租用的虚拟主机进行全生命周期的管理，具体包括：

**1.创建虚拟机**

各部门管理员可以通过创建应用、使用虚拟机模板、自定义方式以及克隆方式创建虚拟机。

**2.销毁虚拟机**

各部门管理员可以通过删除应用来销毁虚拟机，将不再使用的虚拟机销毁，以释放系统资源。

**3.虚拟机操作管理**

各部门管理员可以通过对一个或多个虚拟机，执行启动/唤醒、安全重启、强制重启、休眠、安全关闭和强制关闭等操作。

**4.迁移虚拟机**

各部门管理员可以将虚拟机从一台主机上迁移到另一台主机上。

**5.修复虚拟机**

虚拟机操作系统异常后，各部门管理员可以对虚拟机进行修复。修复虚拟机不会影响用户数据，确保用户信息不丢失。

**6.创建虚拟机快照**

虚拟机快照可保留虚拟机某一个时刻的状态，当虚拟机出现故障时，各部门管理员可以使用快照将虚拟机恢复到创建快照的时刻点。

**7.虚拟机资源调整**

各部门管理员可以根据业务负载调整资源的使用情况，调整虚拟机的 QOS、调整虚拟机 CPU 数目、调整内存大小、增加或修改虚拟磁盘、删除虚拟磁盘、增加或修改网卡、删除网卡、调整虚拟机磁盘的 I/O 上限等。

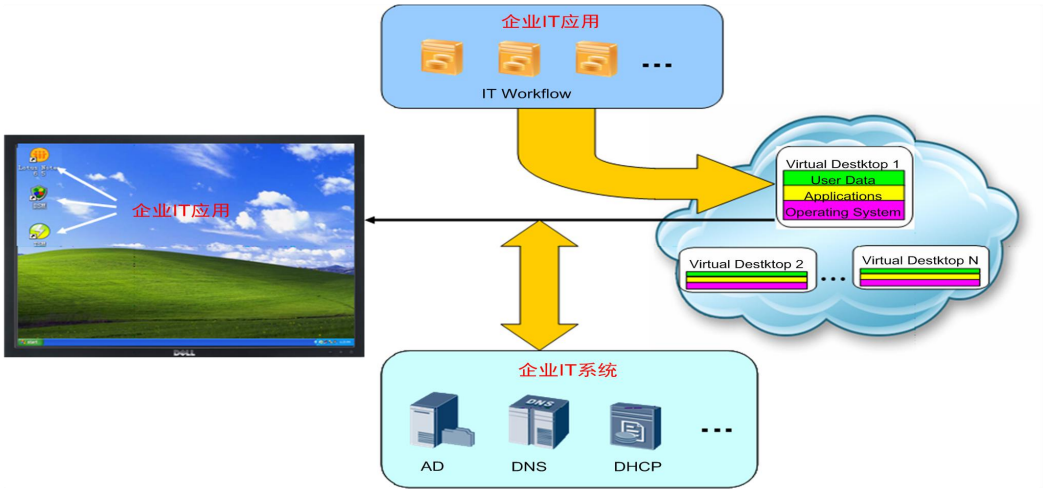
**8.虚拟机性能监控**

各部门管理员可以获取虚拟机 CPU 占用率、内存占用率、网络流速和磁盘 I/O 等信息，还可以按周、月、年及自定义时段查询性能监控结果。

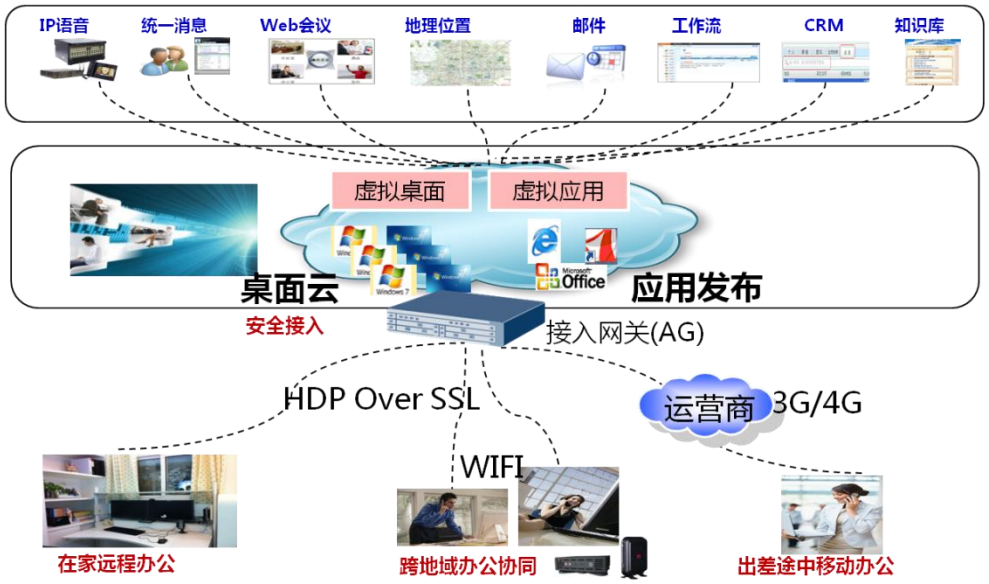
**（四）虚拟桌面服务**

**1.OA 办公虚拟桌面**

OA 办公桌面云是指企业使用桌面云来进行正常的办公活动。桌面云可对接入 USB 设备、打印设备、存储设备进行映射管理；虚拟机里可安装监控软件，提供多种安全方案，保证办公环境的信息安全。




OA 办公用户采用完整复制桌面云。完整复制桌面云基于虚拟机级别的隔离，每个桌面都有单独的系统盘，安全性高、个性化强；外设支持类型丰富，用户体验与传统 PC 一致。每个用户都有一个独立的虚拟机，虚拟机系统盘采用服务器的本地存储，高度集成。用户如果需要扩展存储空间，可增加 SAN 存储。OA 办公的用户与虚拟机采用 1：1 配置，每个人独占一台虚拟机。用户通过本地瘦终端或软终端可以远程登录虚拟机。虚拟机采用业界高保真的 HDP 协议将虚拟机桌面显示投送到用户终端上。瘦终端的无本地存储不涉密、可管控、功耗低，办公环境相对 PC 环境更简洁、无噪音。




基于桌面云的移动办公方案，桌面云与移动终端结合，用户可以在家或非办公室时通过 4G/5G 网络，或通过 WIFI 网络接入桌面云。用户不仅可远程登陆虚拟机，同时也可以通过发布的应用程序进行移动办公，此时用户无需登陆虚拟机直接使用应用，对带宽的要求更低。桌面云支持各种移动笔记本电脑、Pad、手机终端接入，可以实现无缝的随时随地接入进行远程办公，提升效率。

**2. 图书馆阅览室虚拟桌面**

电子阅览室场景中，用户只需要登陆和使用虚拟机，阅览所需要的软件提前安装在镜像中，业务比较简单。电子阅览室主要有如下特点：

（1）可以上网，网络传播的病毒、木马、防不胜防。

（2）人员流动性大，虚拟机无需经常关机。

（3）需要支持外接 U 盘。

（4）维护简单，提高工作效率。

此场景对存储的要求不高，考虑到存在安全威胁，非常适用链接克隆虚拟桌面。链接克隆共用一个只读的系统母盘，这个母盘中安装电子阅览所需要的应用软件。这个母盘不会感染病毒、木马。用户登录使用时，上网、浏览产生的临时数据保存在差分盘中，即使差分盘中了病毒木马。只需要对虚拟机进行重启，差分盘即可清除，还原到系统的初始状态。管理员要对虚拟机进行升级、打补丁，只要更新母盘即可。

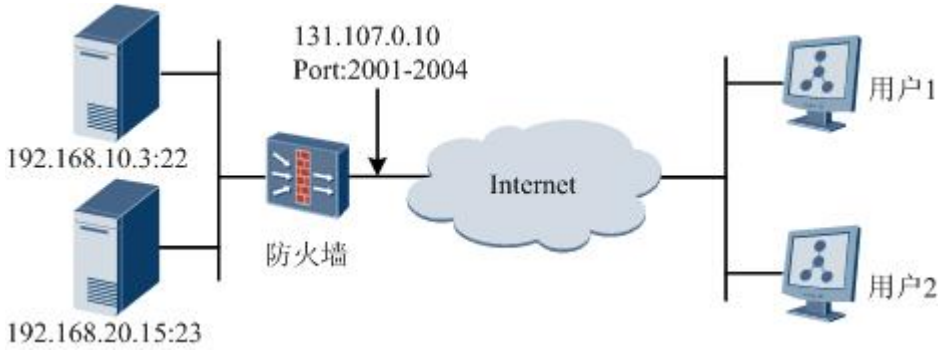
为提高资源复用率，可采用动态多用户方式（动态池）分配给用户。每个 TC 绑定固定的虚拟机账户，开机即可登录使用。流动的用户不用再输入帐户与密码，使用起来非常方便。


**（五）虚拟网络服务**

公共平台可为租用的各部门提供各种网络服务，各部门管理员可以使用公共平台提供的网络服务，根据自己也为需求搭建相应的虚拟网络，实现业务间的互通、隔离、及对外部网络的互联互通等，具体如下：

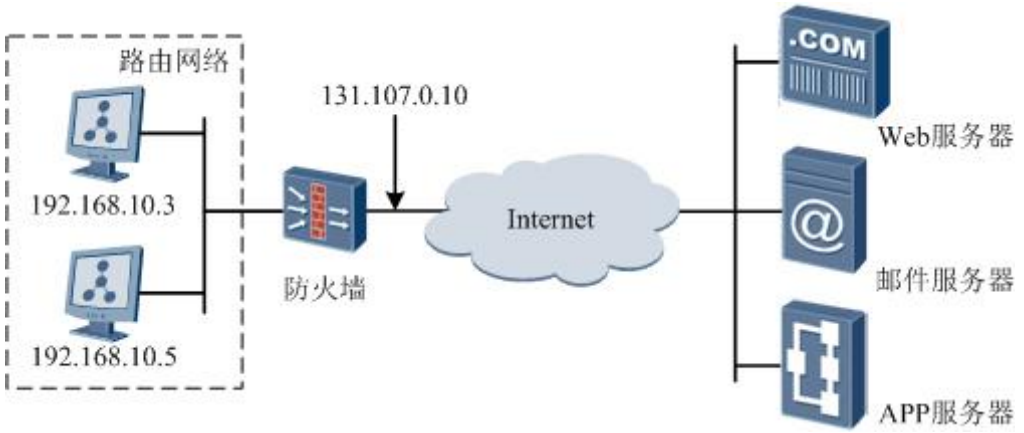
1.DNAT服务

当 VPC 内部需要提供对教师或学生的服务时，通过互联网发起连接请求，由防火墙上的网关接收这个连接，然后将连接转换到内部，此过程是由带有公网 IP 的网关替代内部服务来接收外部的连接，然后在内部做地址转换，此转换称为 DNAT，主要用于内部服务对外发布，如下图所示：




2.SNAT服务

内部地址单向发起请求访问公网上的服务时（如 web 访问），内部地址会主动发起连接，由防火墙上的网关对内部地址做地址转换，将内部 IP 地址转换为公网 IP 地址。这个由网关完成的地址转换称为 SNAT，主要用于内部共享 IP 访问外部，如下图所示。




3.VPN服务

实现将VPN映射到公共平台中为各部门分配的业务资源中。对于公共业务，划分独立的公共业务资源区，并将公共VPN进行映射。

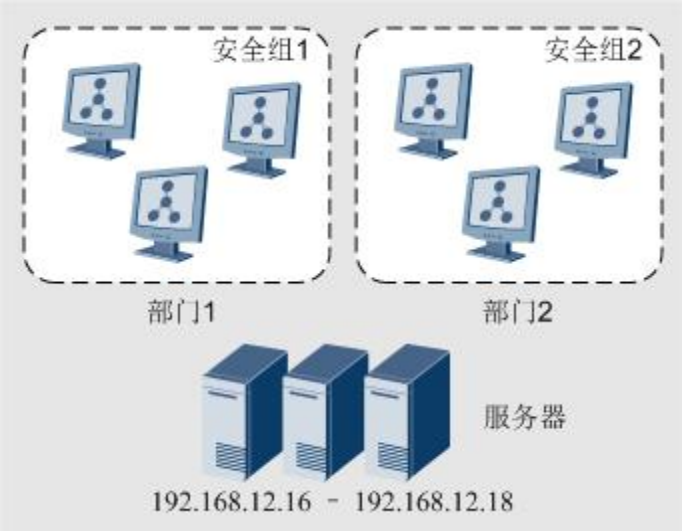
VPN业务用于在公网和学校校园云平台内部网络之上建立一条安全、稳定的通信隧道，各部门的私有业务隔离开来，确保各业务部门的私有业务之间相互隔离，并保证通信隧道内发送和接收数据的安全性。对于公共业务亦实现与部门私有业务之间的隔离。

**4.安全组服务**

安全组用来实现安全组内和组间虚拟机的访问控制，加强虚拟机的安全保护。安全组创建后，管理员可以在安全组中定义各种访问规则，当虚拟机加入该安全组后，即受到这些访问规则的保护。

典型场景举例：虚拟机隔离。例如，在同一VLAN下的两个部门之间相互隔离，同一部门之间的虚拟机可以相互访问，但是所有虚拟机都可以和服务器通信。解决方法如下图所示，分别为部门1、部门2创建安全组1、安全组2，且安全组为组内互通；为安全组1和安全组2添加安全组规则，允许服务器的IP地址段访问安全组。

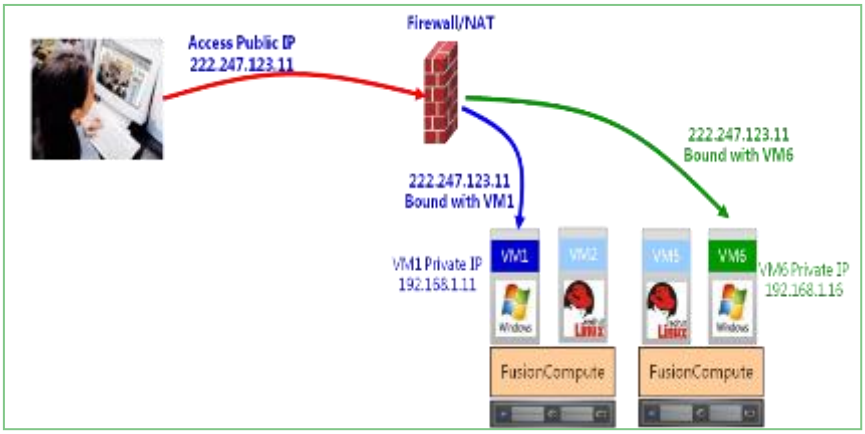
虚拟机隔离如下图：




5.弹性IP服务

对于学校需要对互联网用户提供服务的业务，学校云校园云平台公共服务平台为应用提供弹性 IP 服务。

弹性 IP 地址是一个公网 IP 地址，该 IP 地址可以与各部门 VPC 内部署的应用虚拟机或负载均衡的内部地址进行绑定，从而实现互联网用户的访问。这个内部地址可以是虚拟机的 IP 地址，弹性负载均衡（VLB）的虚拟 IP 地址，或者是浮动 IP 地址。例如，为 VPC 内的 Web 服务器绑定弹性 IP 后，公网用户通过访问弹性 IP 地址使用 Web 服务，如下图所示：



各部门可根据需要调整自己的弹性 IP 对应的虚拟机或负载均衡地址。

**6.弹性负载均衡服务**

学校云校园云平台公共服务平台为各部门应用虚拟机提供负载均衡服务，各部门可以申请负载均衡器，将业务主机关联到负载均衡器中。负载均衡器可以根据用户设定的负载均衡策略，将业务请求均匀分发到相互关联的主机上，使得每个业务主机的负载保持均衡，保证业务运行的稳定性和可靠性。

负载均衡器能够检查服务池中云服务器的健康状态，自动隔离异常状态的云服务器，从而解决单台服务器在处理性能、扩展性、稳定性方面的问题，同时负载均衡器还能起到增强服务器池抗攻击的能力。

弹性负载均衡可以由负载均衡硬件或者负载均衡软件提供。其中，硬件负载均衡器具有高性能、高稳定性、高可靠性、高成本、支持协议多的特点。负载均衡软件属于经济型负载均衡器，具有稳定性差、可靠性低、成本低、支持协议少的特点。

## 四、云平台服务管理

### （一）服务定义

服务中心预置了开箱即用服务，包括 VDC、云主机、云磁盘、物理机等服务，这些预置服务向用户开放所有的服务参数，用户在申请服务时可以选择或输入服务参数，完全由用户自定义所要的服务。例如通过预置服务申请云主机时，

用户选择云主机的硬件规格、操作系统版本，配置云主机的网络。

除了预置服务，全局业务管理员或VDC业务管理员可以根据企业、部门情况，自定义服务目录。例如，全局业务管理员可以定义“标准测试Linux主机”服务，此服务已经固定使用了哪种操作系统类型、硬件规格，甚至云主机所使用的网络、IP地址也是由管理员决定的，用户申请“标准测试Linux主机”时只能输入数量、申请时长，不能由用户决定安装哪种操作系统类型，选择哪种硬件规格。

全局业务管理员或VDC业务管理员在服务定义时，可定义项目包括：

1.服务名称、描述、图标。

2.用户申请服务时可输入哪些服务参数。（例如可以在定义服务时开放云主机规格由用户申请云主机服务时用户自己输入）。

3.管理员审批时可以配置哪些服务参数。（例如管理员收到云主机申请后，可以给云主机配置一个静态IP）

4.锁定某些服务参数，锁定的服务参数在用户申请服务时没有权限配置。（例如定义云主机服务指定操作系统类型为Win7）。

5.配置服务的审批策略：需要审批、不需要审批。

**（二）服务申请**

用户可在自助务门户的服务目录中查看到管理员预定义的各类服务，并根据自己的业务需要选择相应的服务提交申请。申请时可以指定服务的规格参数和使用期限；

各预置服务申请功能列表：

| 服务 | 申请功能 |
| --- | --- |
| 云主机 | 用户可以指定地域、可用分区、操作系统类型、硬件规格、云主机所在网络，云主机个数。 |
| 云磁盘 | 用户可以指定地域、可用分区、硬件规格、存储类型、云磁盘个数。 |
| VDC | 用户可指定配额（CPU 核数、内存、存储、弹性 IP 个数、VPC 个数、安全组个数、虚拟机个数）、VDC 可使用哪些资源池。 |
| 弹性 IP | 用户可以指定地域、VPC、弹性 IP 个数，当前采用硬件路由器时，可以指定规格、公网 IP 池。 |

**（三）服务审批**

VDC 业务管理员可以审批来自 VDC 内用户提交的服务申请，全局业务管理员可以审批来自 VDC 业务管理员提交的 VDC 服务申请。审批时，审批者可以选择“同意”或者拒绝外，还可以配置一些服务参数，例如虚拟机所使用的网络（审批者可以配置哪些服务参数可以在定义服务阶段配置）。

**（四）服务维护**

业务用户可以对已申请服务进行维护操作，例如 VNC 登录虚拟机、虚拟机上/下电，虚拟机绑定弹性 IP，磁盘绑定虚拟机。

各服务维护功能列表：

| 服务 | 维护功能 |
| --- | --- |
| 云主机 | 云主机上/下电、重启、休眠、云主机转虚拟机模板、VNC 登录、查看监控信息、创建云主机快照。 |
| 云磁盘 | 云磁盘挂载到云主机，或从云主机上卸载。 |
| 弹性 IP | 弹性 IP 绑定到云主机或负载均衡器，或从云主机、负载均衡器解绑定。 |
| VDC | 查看 VDC 配额使用情况，VDC 下已申请资源列表，资源数量统计。 |
| VPC | 查看 VPC 网络拓扑，在 VPC 下管理网络、路由器、防火墙、安全组、弹性 IP、负载均衡器、VPN、DNAT。 |

### （五）服务变更

对于已发放的资源，用户可以提出变更申请对服务参数进行变更。用户可以申请将一台已发放的 4G 内存的虚拟机变更为 8G 内存。

服务变更功能列表：

| 服务 | 变更功能 |
| --- | --- |
| 云主机 | 变更云主机硬件规格、服务到期时间。 |
| 云磁盘 | 变更块云磁盘规格、服务到期时间。 |
| VDC | 变更 VDC 的配额、服务到期时间。 |
| 弹性 IP | 服务到期时间。 |

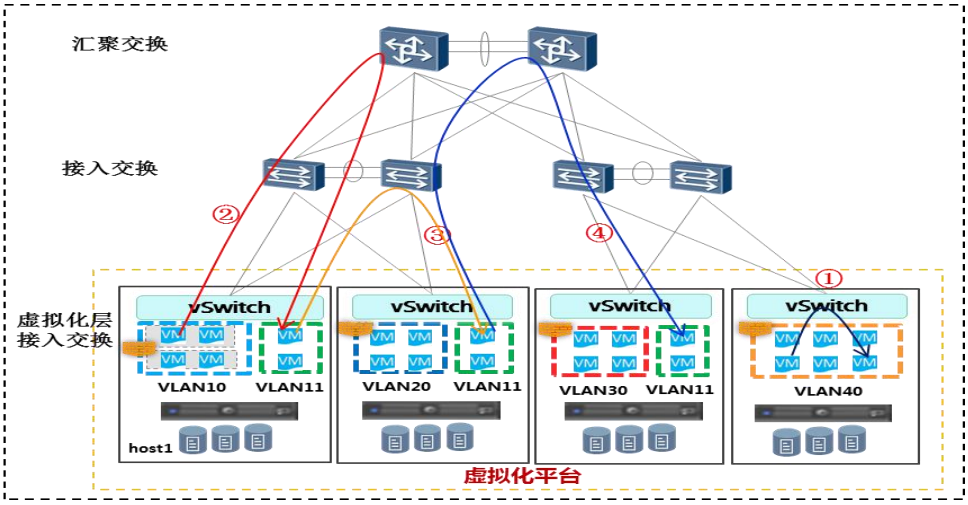
### （六）服务释放

对于不再使用的资源，用户可以提出释放申请，系统会自动释放用户的资源。也支持服务到期后，由管理员释放资源。对于到期的服务，业务用户和 VDC 业务管理员登录到租户 Portal 后，会收到到期提醒。对于已经到期的 VDC，用户无法从 VDC 服务目录下继续申请服务。

## 五、虚拟化安全隔离

### （一）虚拟机 VLAN 隔离

虚拟机之间可以采用 VLAN 隔离的方式，保障各虚拟机之间的网络交互安全性和可控制性。




具体隔离策略可参考如下规则：

1. 同一虚拟交换机内同一 VLAN 通信：不出虚拟交换机，直接在虚拟交换内部完成交换；

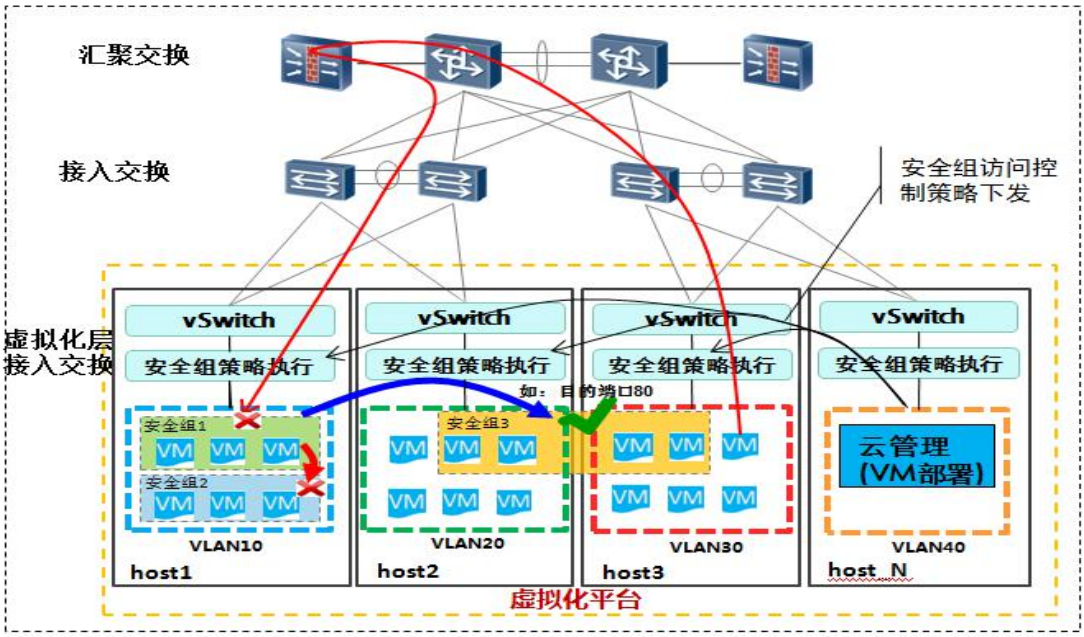
2. 同一虚拟交换机内不同 VLAN 通信：通过外部三层互通网关完成 VLAN 间互通；

3. 不同虚拟交换机间同一 VLAN 通信（同一物理接入交换机内）：通过物理接入交换机二层互通；

4. 不同虚拟交换机间同一 VLAN 通信（跨物理接入交换机）：同 2，通过外部三层互通网关完成 VLAN 互通。

**（二）虚拟机安全组隔离**

VPC 安全组，可对虚拟机设置灵活的访问权限控制。




安全组：具有相同的安全策略的一组 VM 的集合,支持安全组间的访问控制策略和安全组内成员间的互访策略。每个 VM 一组 ACL，互不影响，VM 迁移时安全策略自动刷新。提供 VM 粒度的隔离机制，解决 VLAN 资源不足、配置工作量大的问题。

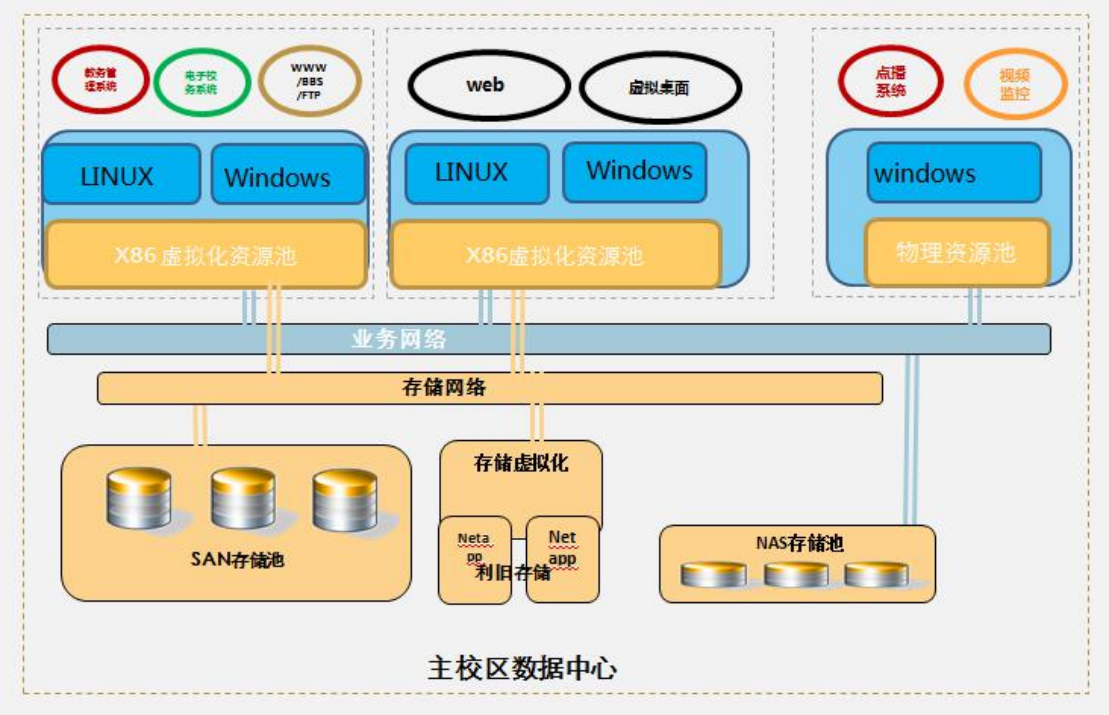
分布式策略控制，报文无需迂回到集中的策略控制点，避免形成性能瓶颈。可以和边界防火墙共同部署，构筑立体安全防护能力（南北向流量控制+东西向流量控制）。

## 六、存储资源池设计

### （一）存储资源池设计

存储系统应采用先进、成熟的技术和优良的系统设计，使系统在整体上具有很快的响应速度和更高的数据带宽，可长时间承受大量用户极高的访问频率和访问速度。在系统设计中，应切合云主机应用，将不同特点的数据均存储在大型集中的的存储设备中，使整个存储系统具有高可靠性、异构平台共享、高性价比、可扩展、易管理、易使用、性能优良

等一系列优势，并能平滑地升级扩展，很好地适应数据存储技术的发展，满足学校的中长期发展的数据存储需求。

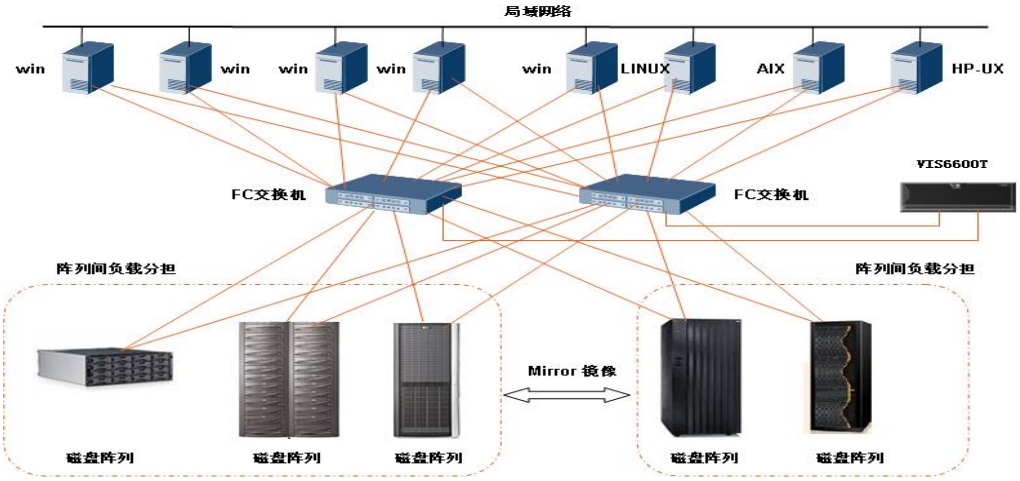



当前虚拟主机数量及类型多，要求存储系统能够提供非常好的兼容性将主机各应用系统接入；应用系统和操作系统差别很大，要求存储系统必须提供统一的数据保护方案，简化方案的部署和维护；存储设备比较多，要求建设方案能够将现有和新增的存储设备进行统一的管理、配置、数据保护和存储应用。业务扩展需求，要求系统必须是一个开放的平台，能够在线扩展存储容量和应用，能够平滑升级存储数据保护层次。

鉴于本项目复杂的现网情况和丰富的业务需求，存储与计算分离，虚拟化平台业务存储采用 FC SAN 连接主存储阵列。通过虚拟化集中部署，动态分配和调用资源，实现计算和存储资源的高效管理。同时对于核心业务数据通过镜像卷

技术实现本地存储高可用，以及后续的双数据中心容灾的平滑演进。对于非结构化数据的多媒体应用业务，存储采用 NAS 存储提供高带宽、高并发的文件共享服务。

### （二）异构存储整合




基于 VIS6600T 的虚拟化方案拓扑

在生产中心 SAN 架构网络层需要加入虚拟化智能设备一台，实现对异构存储系统的整合和统一管理。

存储虚拟化是基于存储网络的虚拟化，通过为数据管理系统提供了一层虚拟的“卷”的逻辑设备，来屏蔽异构存储设备的差异，并通过对逻辑卷的管理，克服硬件设备的物理局限性和差异性，使逻辑卷可以跨越多个物理磁盘。另外，存储虚拟化能在系统处于活动状态时动态配置磁盘存储区。

存储虚拟化可以完成对于客户处所有阵列的统一管理以及统一数据保护，大大简化了网络架构、提升了工作效率。客户处原有阵列常常需要分散管理，耗费较多人力和精力。部署完存储虚拟化以后，可以实现多台阵列的统一管理，节约了管理成本，简化了管理难度。

为保证虚拟化前后数据状态的一致性，存储虚拟化通过一系列保障技术，能够使得虚拟化后的数据与虚拟化之前的数据状态保持一致，这就避免了虚拟化过程中复杂的数据迁移和恢复过程，不仅大大简化了虚拟化的实施，而且减少了系统的停机时间，提高了业务的连续性。

存储虚拟化能够在线扩展存储容量和应用，客户处新增存储阵列或者新增业务主机可轻松加入现有网络,实现系统平滑升级。

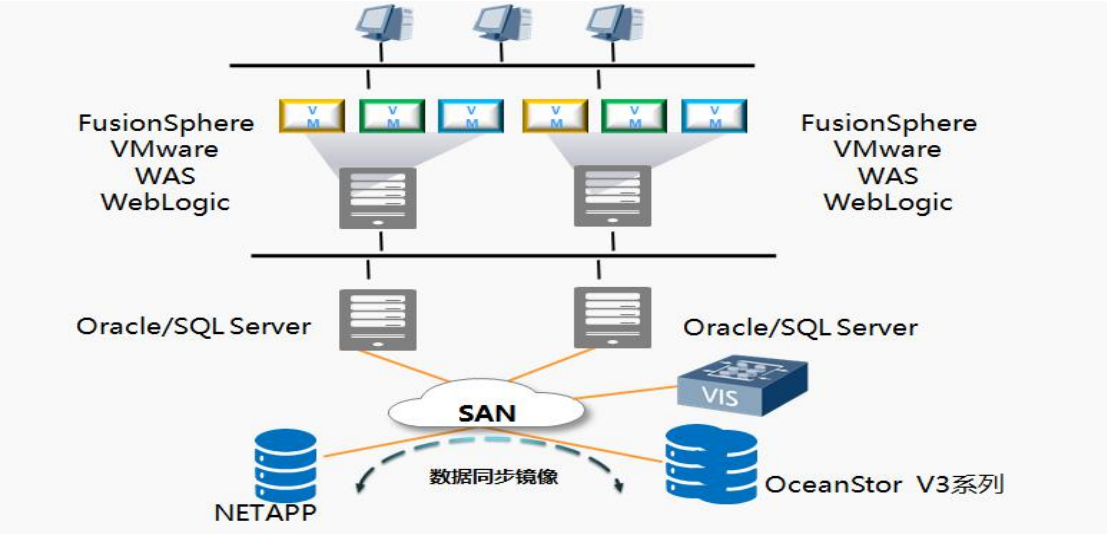
同时，存储虚拟化产品可以提供丰富的数据管理功能，这些功能可以适用于存储虚拟化管理的所有存储系统。主要可以提供的软件特性列举如下：

1.提供高级的数据复制功能：能跨多种存储系统复制数据，实现同城或者跨越城市的远距离容灾解决方案。

2.提供高级的远程镜像功能：利用远程镜像功能，可实现基于 FC 通道的同步远程容灾解决方案。

**（三）本地高可用保障**

本地高可用解决方案通过存储虚拟化和卷镜像技术，实现存储的高可用部署，结合主机层集群技术来实现业务连续性本地高可用解决方案，当故障发生时，确保备用服务器，备用网络和备用存储能快速自动的实现业务的冗余访问。避免但设备故障引发的业务长时间中断。




应用层通过主机集群或者应用程序集群实现高可用组网，当任一主机故障之后应用自动切换到其他主机。应用主机安装多路径软件，提高数据传输的可靠性，保障应用主机与存储阵列之间的路径安全性。

存储层通过冗余的 FC 交换机、VIS 虚拟化网关的异构虚拟化特性实现阵列间数据同步镜像，达到高可用组网。当任一交换机、磁盘或者存储阵列故障，不影响主机应用。

## 七、统一运维管理平台

数据中心综合运维管理针对的主要问题是资源利用率低下、运维效率低下、维护成本高、业务上线慢、系统故障频发等。为此需要实现的主要目标是运维自动化、便捷化、低成本、高效率，以及高可靠和高可用。

云数据中心运维管理平台提供一站式解决方案，把物理分散的多数据中心资源整合为逻辑统一的资源池；把计算、存储、网络等基础架构资源作为云服务向用户提供；实现了用户自助服务；数据中心物理资源和虚拟资源统一调度，自

动化控制和部署；流程化、标准化的对云服务进行统一监管维护。

**（一）统一运维管理平台通过对老校区数据中心资源的统一管理达成如下目标：**

**1.提高资源利用率，降低总所有成本**

整合现有数据中心资源，将多个物理分离的数据中心整合为逻辑上统一的大资源池。在统一资源池内统一分配和调度位于不同数据中心的资源。资源分配时，可以按业务资源使用量进行调度。对物理资源池、资源分区，做资源碎片整理，避免盲目资源扩容。

**2.业务敏捷，缩短业务上线时间**

通过服务目录、自助服务，业务部门可以自助、快速的申请资源；通过所见即所得的服务编排，快速定义业务运行需要的计算、网络、存储等环境模板；根据模板，能够实现资源的自动化控制，使业务所需资源可以及时获取。

**3.创新服务模式**

基于各部门或业务单元对资源使用进行计量、统计，为各部门或业务单元分担资源成本提供依据。

**（二）统一运维管理平台的系统功能要求**

**1.云服务运营**

为用户提供统一的自服务门户，用户在门户中可以进行服务申请、资源管理、资源操作等。

为管理员提供管理门户，门户的主要功能包括服务定义、订单审批、服务流程编排、用户管理、资源管理、模板管理、资源和运营报表等。

**2.服务运维**

基于 ITIL V3 最佳实践，提供事件管理、配置管理、发布管理、变更管理、容量管理、CMDB 等功能。

**3.维护中心**

提供多数据中心全局统一的监控、告警管理、性能管理。是数据中心日常运维的门户。

**4.资源池管理**

接受服务运营模块的资源服务请求，实现本地资源的分配调度，并对计算、存储、网络等设备做自动化控制、部署，以提供满足业务要求的运行环境。

实现数据中心本地资源的自动发现、自动化控制，通过监控感知资源状态、资源负载，并根据策略对资源做动态调整。提供本地管理 Portal，实现本地资源配置、模板管理、镜像管理。

**（三）统一运维管理平台的使用价值要求如下：**

**1.易于使用**

系统本身具有直观、易理解的操作界面，让用户第一眼就能找到自己最关注的功能操作和数据信息。操作步骤、结果不违背多数人的常识和常规意识，并提供详细的帮助信息。

UI 界面分角色，呈现用户角色关心的信息，少部分用户使用的高级特性通过选项方式呈现。90%以上的任务操作小于 3 步，超过 5 步的操作采用导航的方式。

要让系统总是在合理的时间反馈给用户合理的信息，而不是让用户等待，操作响应小于 3 秒。

**2.统一门户**

统一管理门户提供了各类管理子系统的单点登录入口，也提供集成客户已有管理系统入口的能力。

**3.统一管理**

支持对单个或多个分布式数据中心内的物理和虚拟资源进行统一管理。

**4.灵活定制**

支持通过插件方式，实现南向接口能力扩展、和客户已有 IT 管理系统进行对接。

服务目录、资源模型、资源视图、调度策略等，支持客户自定义，通过插件扩展调度策略、服务类型。支持资源和服务的灵活编排，统一调度计算、存储、网络资源。

可视化流程设计，通过插件扩展流程节点，满足灵活多样的用户服务请求和配置策略。

**5.平滑扩展**

系统按照高性能、大容量原则设计，提供平滑可伸缩的系统架构，支持高并发量用户访问，具备良好的扩展性。

**6.开放标准**

系统采用 SOA 架构，提供开放的 API，易于跟第三方系统集成对接；采用开放的体系架构，遵循国际标准、行业标准，能够适应业界主流的操作系统、Web 中间件、数据库等，保证系统能够随时无障碍地进行更新和移植。

**7.组件化、松耦合**

系统各部件之间松耦合，功能部件间的升级、变动不影响其他组件。

**8.高可靠**

统一运维管理平台具备高可用性、高可靠性。采用高可用双机技术、流量控制及过载保护机制，从硬件、网络、软件等各层次进行系统可靠性系统架构设计，保证系统能够提供高性能的数据处理和应用响应能力，确保各类应用系统和数据库的高效运行，承载大量的用户访问。

## 八、云平台可扩展性

### （一）主机可扩展性

云平台中每个资源管理平台最大支持 256 个 VRM 集群，4096 个主机服务器、80000 个虚拟机支持。每 VRM 集群支持的服务器数量最大可达到 256 台，每 VRM 集群支持 32 个 HA 资源池。每 HA 资源池内支持的服务器数量最多可扩展至 128 台服务器，可轻松满足未来桌面的平滑扩容需求。

单虚拟机可扩展性设计：单虚拟机支持 VCPU 个数最大可以扩展到 64 个，内存可以扩展到 1024GB，支持的虚拟网卡数最多可以支持 12 个，可充分满足虚拟机规格的弹性伸缩。

**（二）虚拟桌面扩展性**

虚拟桌面管理节点可分布式平滑扩展。一套虚拟桌面最大支持 20000 桌面用户，当超过 20000 用户容量后，需要新增加一套虚拟桌面管理节点，虚拟桌面管理节点之间属于分布式，相互之间完全独立。

**（三）存储扩展性**

根据存储需求增长，可以实现存储在线平滑扩容，根据规划可以在线扩展磁盘、磁盘框、控制框。资源管理平台支持存储冷热迁移，支持将虚拟机的存储卷在同一套存储中的不同 LUN，或者两套不同存储之间进行迁移；满足客户存储进行平滑扩容的需求。