

易讯通

云管理平台解决方案

北京易讯通信息技术股份有限公司

2016年5月

目录

1 总论

1.1 概述

1.2 建设背景

2 需求分析

2.1 客户现状

2.2 客户需求

1) 提高运维管理效率，降低成本

目前管理维护人员都是进入机房，在机架旁操作服务器，但由于各主机都有自己的维护界面，造成系统维护人员需要逐个进行维护管理，显然这种单点式的维护需要耗费大量的人员成本，且效率很低。

2) 提升数据中心安全性

通常在出现问题的情况下，可能进入机房进行查看与维护，而由于各系统的数量及种类在不断增加，以往单一的管理模式已经不能满足数据中心发展的需求，需要一个统一的管理门户来对数据中心进行管理维护，且在整个过程中，保证公安系统的安全，做到一站式的授权、认证，操作，审计。

3) 业务保密性、可用性，稳定性

公安系统相关涉密系统都需要特别管理，对其上所载的业务要做到安全、稳定，可用。尤其在特殊服务器出现宕机等情况下，不能及时的连接或查看相关故障，延误了时间，可能会造成损失，这就需要做到服务器主机的高可用，高稳定，高安全。

4) 提升整体办公及运维安全性

在公安系统中，内外电脑用于各种日常办公业务的开展，外网电脑用于信息资料的采集，从内部管理上，严格禁止“一机两用”，且在运维管理上，由于大多采用的是传统的PC电脑形式，有些可能已经服役较长年限，如何保障日常办公的正常开展，以及内外网的专网专用，提升整体办公水平以及运维安全。

5) 专网专用，在安全的前提下满足业务和管理需求

一机一用，禁止“一机两用”，从根本上杜绝可能发生的数据风险。通常，安全来自外部或内部的侵袭，而来自内部的数据损坏，更需要我们采用更加有效的手段来规避，在保证安全的前提下，满足公安系统人员的办公和业务需求。

6) 信息安全、可控性

随着国家将信息化和信息安全作为国家发展的最高战略方向，作为公安系统，建设“安全可控”的业务系统安全体系，有着非常重要的战略意义，尤其是在涉密网，保证数据的绝

对安全。为了避免潜在的安全隐患，使用自主可控的国产软硬件产品和服务，把信息安全掌握在自己手中，确保信息安全，打造一个安全可信的计算机环境。

7) 虚拟桌面的高可用性，满足业务持续性。

在硬件服务器或虚拟机桌面发生意外的情况下，通过高可用功能，在无人工干预情况下，自动将发生故障的服务器或虚拟机系统在其他服务器上重新启动，保证员工工作的持续性。在零客户端发生意外故障的情况下，只需在短时间内更换一台零客户端即可恢复业务操作。

3 建设方案

3.1 总体架构及组成

本次方案设计采用易讯通拥有完全自有知识产权的云产品——ECloud云管理平台。

ECloud云管理平台以高性价比实现云计算的完整解决方案（即IaaS、PaaS服务），对虚拟机、主机集群、存储、网络等资源及上层应用系统进行统一的自动部署、监控和资源调度、统一分配管理。不仅降低系统复杂度与成本，实现资源的最大化利用与服务的最快交付，也改善了IT资源的使用效率和管理能力以及最终用户获取IT资源的能力。

ECloud云管理平台从服务的角度出发，关注如何满足上层业务应用的需要以及如何将资源封装为可度量的服务，内置丰富的资源管理与交付功能，为用户提供简单、统一的集中管理平台。使用ECloud云管理平台将原本静态分配的IT基础设施抽象为可管理、易调度、按需分配的资源；把资源的能力封装对外提供按需灵活使用各类IT资源的服务，并提供运营管理等功能，帮助运营者完成日常运营工作，面向最终用户提供自助服务流程，使最终用户以最便捷灵活的形式按需使用这些服务，满足安徽移动统一业务生产环境管理平台的运营。

3.1.1 系统架构图

ECloud云管理平台由资源池层、适配层、控制层、管理层和服务层构成。

资源池层：数据中心的基础设施，包括计算资源、存储资源和网络资源。

适配层：ECloud云管理平台兼容各种虚拟化技术，对虚拟化平台统一管理调度，对计算、存储、网络等物理资源进行池化，抽象成可管理、可调度的逻辑资源，兼容异构虚拟化平台调用接口，向上提供一致化的访问。

控制层：包括云运维管理平台的各个功能模块，例如资源管理、资源运维、资源调度等功能，提供了一系列自动化运维功能，降低了传统人工运维的成本，提高了云数据中心的运维质量和效率。

管理层和服务层：ECloud云管理平台在整合底层资源，提供运维手段的同时，也对外提供一系列服务。这些服务由管理层进行统一管理，服务层提供对外接口。

门户：云管理平台为用户提供完全透明的计算及存储资源，用户的应用系统可通过远程接入方式在云管理平台所提供的计算资源上（虚拟服务器和物理服务器）直接进行部署、应用，而无需关心其底层架构。

3.1.2 存储架构设计

存储系统采用共享式存储和分布式存储并存；FC SAN和IP SAN兼顾方式，满足不同存储方式需求；并提供业务数据备份功能，共享式存储和分布式存储统一在云平台管理、展现、运营。

3.1.2.1 分布式文件存储

分布式文件存储系统能给用户带来更高的性能、扩展性和可用性。从文件系统的客户使用的角度来看，它就是一个标准的文件系统，提供了一系列API，进行文件或目录的创建、

移动、删除，以及对文件的读写等操作。从内部实现来看，分布式的系统则不再和普通文件系统一样负责管理本地磁盘，它的文件内容和目录结构都不是存储在本地磁盘上，而是通过网络传输到远端系统上。并且，同一个文件存储不只是一台机器上，而是在一簇机器上分布式存储，协同提供服务。

系统架构如下图示：

分布式文件存储系统架构图

底层存储层基于分布式文件系统实现，负责数据切片，数据存储，并提供相应状态信息，具体存储方式对外部应用透明。

业务层实现了文件、目录、访问权限相关的具体功能，具体包含了文件访问、文件属性、目录访问、目录属性、ACL认证鉴权等业务模块。

接口层为上层用户应用系统以及资源池管理平台提供基于 NFS、CIFS等符合 POSIX标准的文件系统接口。支持多租户管理及访问权限设置。系统通过负载均衡实现多台设备为业务系统提供统一的高效数据访问，避免单接入点网络和性能拥塞。

3.1.2.2 弹性块存储

云管理平台通过存储适配器和不同厂家的存储设备对接，采用存储设备管理软件提供的功能接口实现管理，将多个存储设备的资源整合在一起并抽象化，对外提供整体的出口和存储空间管理，让它看上去如同一个资源。

存储资源池可以由含有虚拟化能力的存储设备（如分布式文件存储系统、虚拟化存储）来承建。通过存储设备提供的接口，资源池管理模块可进行存储类资源的容量管理，支持对挂载到虚拟机的存储容量的划分和管理。

系统架构如下图示：

存储层实现块存储的功能。对外暴露块存储协议（如 iSCSI协议）。块存储资源在物理形态上可以是基于硬件的存储设备，如 IPSAN设备，也可以是运行有 iSCSI软件的存储型服务器。

服务层负责对块存储资源的管理，并向资源管理平台和虚拟机系统提供 API。对资源管理平台提供的 API 能力包括：卷操作和业务计量信息上报，与虚拟机系统交互的 API 主要是存储 Mapping 配置。

块存储系统提供虚拟机实例使用的数据块级的存储卷，高可靠性的存储卷可以附加到一个正在运行的虚拟机实例，作为一个实例内的设备。EBS是特别适合于应用程序需要一个数据库，文件系统，或原始块级存储访问。块存储系统为用户提供块级别的高速数据存储服务的存储系统，用户可使用块存储设备在虚拟机或物理机上以卷的方式存取数据。

管理平台的 FC-SAN块存储系统允许您创建存储卷从 1GB到 2TB，可作为设备安装到虚拟机实例，多个卷可以安装到同一虚拟机实例下。

实现方式

云管理平台将提供给虚拟机使用的一块存储空间称为一个卷。卷既可以是系统盘也可以是数据盘，也通常作为引导盘使用。每个虚拟机都有一个系统盘和一个数据盘，数据盘提供额外的存储空间。用户可以将多个数据盘挂接在一个虚拟机上。这些数据盘可以从管理员提供的存储服务中获得。

需要指出：卷和 Hypervisor 种类相关：一种 Hypervisor 的卷不能供另一种 Hypervisor 使用。

块存储系统非常适合数据库，以及需要运行文件系统或者访问原始块级存储器的许多其他应用程序。在开始和停止虚拟机实例时，将会以与传统物理服务器非常相似的方式维持那些保存在数据库或应用程序中的信息。

块存储系统的目的是让虚拟机的用户附加存储卷的任何实例。如果虚拟机实例启动失败，用户的 EBS卷自动分离，保证用户数据完好无损，然后，用户可以重新装上卷到一个新的实例，并迅速恢复数据。

存储卷就像原始、未格式化的块设备，为用户提供设备的名称和块设备接口。资源池管理平台的 EBS卷上，用户可以创建一个文件系统，或以任何其他方式如：使用一个块设备（如：硬盘驱动器）的方式来使用它们。

资源池管理平台的 EBS卷放置在一个特定的可用性区域，然后可以连接实例到同一可用性区域。

块存储系统还提供了创建时间点的快照，这些快照可以被用作新的 EBS卷的起始点。

块存储系统提供的备份在某时间点的快照。FC-SAN块存储系统的快照增量备份，这意味着，只有自用户上次快照后发生改变的设备块将被保存。如果有一个 100GB 的数据的设备，但只有 5GB 的数据已经改变，因为最后一个快照，只有 5 个额外的 EBS快照数据将被存储到二级存储。当用户删除一个快照时，只有不为任何其他快照所需的数据将被删除，所以，不管这之前的快照是否已被删除，所有活动的快照将包含所有需要恢复卷的信息。

块存储系统使用非常简单，但提供无限的选择：快照、可用性、性价比，并提供大量的自动化。毫不夸张地说，块存储系统带来云计算的一个全新的水平。

3.1.2.3 对象存储

对象存储系统提供 HttpWeb 访问服务，以 Restful 方式提供给应用开发，兼容亚马逊的 S3 和 Swfit。其核心就是将任何类型的数据当作对象，存储到对象存储提供的空间中。用户可以写入、读取、删除、复制存储空间中的任意对象。同时可以控制存储空间的访问权限、查看该存储空间的访问日志及其对象。向用户提供各种类型数据的存储、访问、备份、共享等管理功能。应用场景包括：网盘应用、存储备份、海量数据存储、BigData 分析、HPC 数据处理。

基于对象的分布式存储系统的由接口层、服务层、存储层和系统管理模块构成。接口层通过负载均衡和 WEB 服务为用户应用系统及资源池管理平台提供基于 HTTP 协议的对象存储服务。服务层实现对象、容器及用户相关的具体功能。存储层使用基于 X86 架构服务器集群的分布式存储系统实现数据的存取。分布式存储系统提供容器信息、对象内容和对象属性所需要的存储空间和相关存储机制及元数据信息。

系统管理是分布式存储系统内部进行运维的管理控制单元，同时实现资源池管理平台接口实现。系统管理包括计量信息、用户控制、日志管理、统计报表和运维管理等模块。通过对象存储系统为客户提供可按需扩展的文档存储空间，用户可对任何类型的文档进行上传、下载、删除等操作。

3.1.3 网络架构设计

系统组网图

3.1.3.1 系统组网说明

整个业务云系统网络采用大二层结构设计，资源设备由接入交换机直接连到核心交换，取消传统三层架构中的汇聚层。如上图所示，系统的网络构架分为运营管理层、业务层、核心层及网络出口层，以下详细介绍每一层的功能和特点：

业务层

业务层提供了各类应用所需的计算、存储资源，并将这些资源接出到外部。业务层的通过资源的分类，又将网络划分为三个区域：主存储、二级存储、计算资源。根据不同应用对各类资源的不同需求，实现资源的按需分配和动态调度。

基于统一平台的原则，计算资源均采用 X86 平台，主存储可使用 IPSAN 或 FCSAN, 二级存储可使用分布式 NAS 设备。

核心层

核心网络层需要支撑整个系统的数据交换和传输功能，是决定系统网络性能的关键区域。

运营管理层

运营管理层配备一台 X86 服务器，在其上部署虚拟化软件，再将云平台部署在虚拟化硬件上。

网络出口层

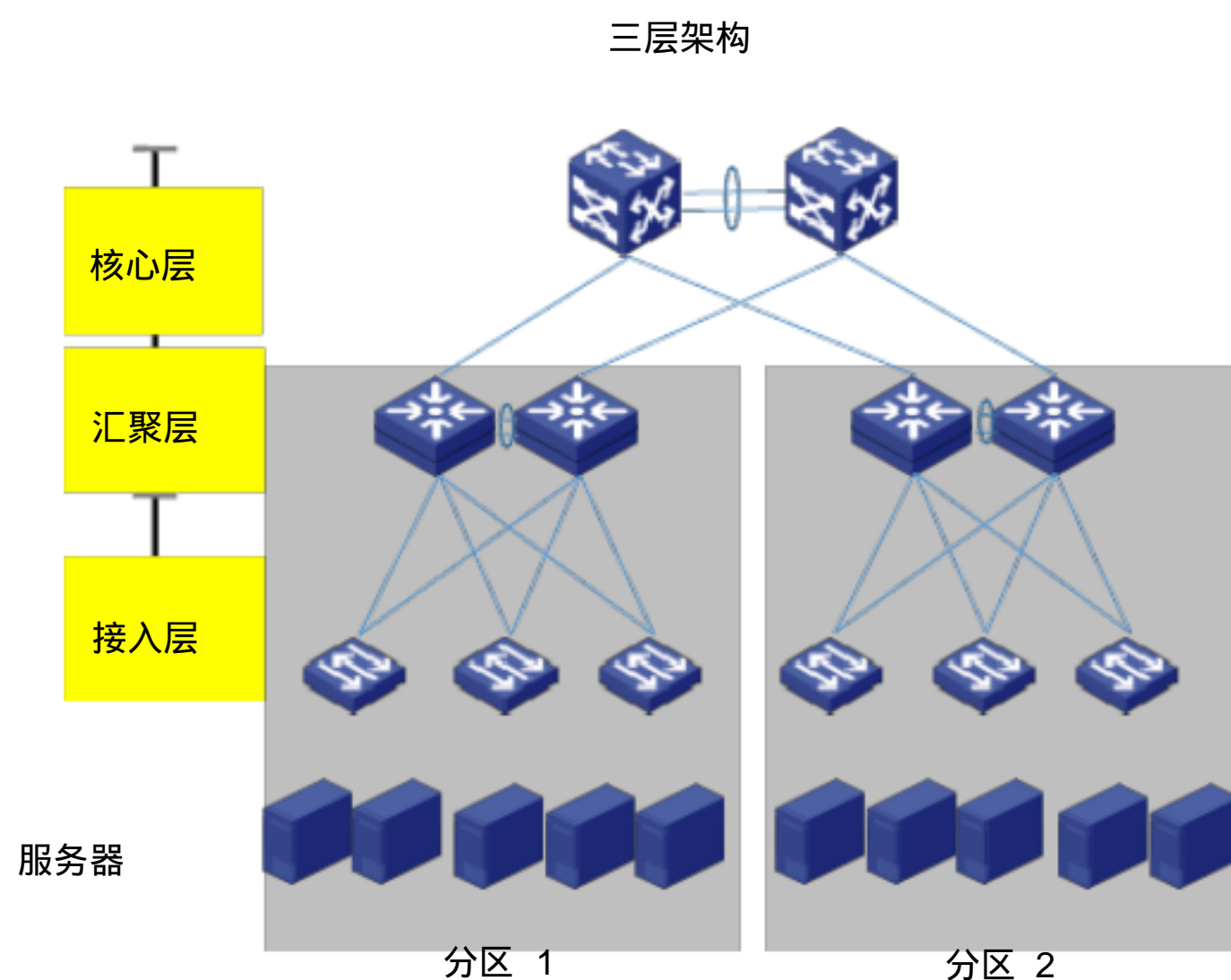
通过双网络出口和万兆光纤接出。

虚拟机网络

事实上，业务云系统中还有另外一个网络平面—虚拟机网络。业务系统运行在虚拟机上，众多的业务虚拟机组成了一个虚拟机网络平台。根据不同的业务需要，虚拟机需要通过 VLAN 来相互隔离，起到多租户，多业务安全作用。

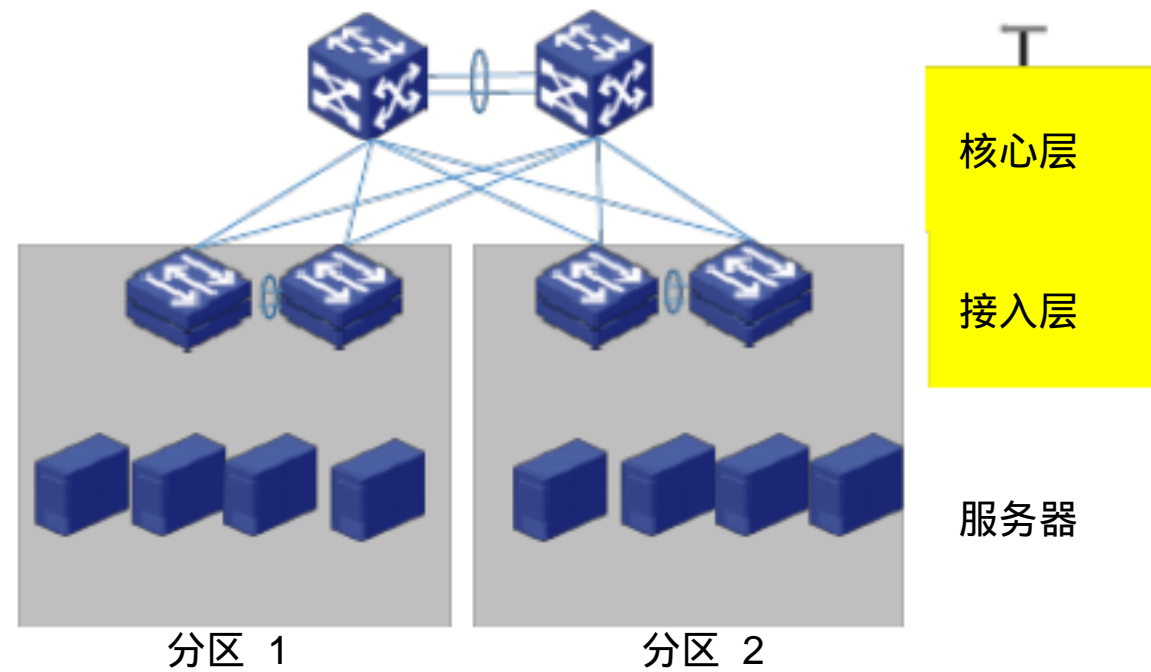
3.1.3.2 网络方案亮点

3.1.3.2.1 二层网络架构



传统的网络方案一般采用接入、汇聚、核心三层架构。三层架构下可以保证网络具备很好的扩展性，同一个分区内服务器接入密度高。但三层架构网络设备较多，不便于网络管理，运维工作量大。同时组网成本相对较高。

二层架构



随着交换机的端口接入密度也越来越高，二层组网的扩展性和密度已经能够很好的满足绝大多数服务器接入的要求。在服务器虚拟化技术应用越来越广泛的趋势下，二层架构更容易实现 VLAN 的大二层互通，满足虚拟机的部署和迁移。相比三层架构，二层架构可以大大简化网络的运维与管理

3.1.3.2.2 DMZ 区划分

DMZ(DemilitarizedZone) 即俗称的非军事区，与军事区和信任区相对应，作用是把 WEB,e-mail,等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。DMZ 可以理解为一个不同于外网或内网的特殊网络区域，DMZ 内通常放置一些不含机密信息的公用服务器，比如 Web、Mail、FTP等。这样来自外网的访问者可以访问 DMZ 中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使 DMZ 中服务器受到破坏，也不会对内网中的机密信息造成影响。

当规划一个拥有 DMZ 的网络时候，我们可以明确各个网络之间的访问关系，可以确定以下六条访问控制策略。

内网可以访问外网

内网的用户显然需要自由地访问外网。在这一策略中，防火墙需要进行源地址转换。

内网可以访问 DMZ

此策略是为了方便内网用户使用和管理 DMZ 中的服务器。

外网不能访问内网

很显然，内网中存放的是公司内部数据，这些数据不允许外网的用户进行访问。

外网可以访问 DMZ

DMZ 中的服务器本身就是要给外界提供服务的，所以外网必须可以访问 DMZ。同时，外网访问 DMZ 需要由防火墙完成对外地址到服务器实际地址的转换。

DMZ 不能访问内网

很明显，如果违背此策略，则当入侵者攻陷 DMZ 时，就可以进一步进攻到内网的重要数据。

? DMZ 不能访问外网

此条策略也有例外，比如 DMZ 中放置邮件服务器时，就需要访问外网，否则将不能正常工作。在网络中，非军事区 (DMZ)是指为不信任系统提供服务的孤立网段，其目的是把敏感的内部网络和其他提供访问服务的网络分开，阻止内网和外网直接通信，以保证内网安全。在本方案中采用防火墙设备提供的虚拟防火墙实现。虚拟防火墙是一个逻辑概念，可以在一个单一的硬件平台上提供多个防火墙实体，即，将一台防火墙设备在逻辑上划分成多台虚拟防火墙，每台虚拟防火墙都可以被看成是一台完全独立的防火墙设备，可拥有独立的管理员、安全策略、用户认证数据库等。每个虚拟防火墙能够实现防火墙的大部分特性。每个虚拟防火墙之间相互独立，一般情况下不允许相互通信。

SecPath/SecBlade 虚拟防火墙具有如下技术特点：

每个虚拟防火墙维护自己一组安全区域

每个虚拟防火墙维护自己的一组资源对象（地址 /地址组，服务 /服务组等）

每个虚拟防火墙维护自己的包过滤策略

每个虚拟防火墙维护自己的 ASPF策略、NAT策略、ALG策略

限制每个虚拟防火墙占用资源数：防火墙 Session以及 ASPFSession数目

虚拟防火墙预先定义了四个安全区域，这些安全区域也称为系统安全区域，分别为 Local 区域、Trust 区域、Untrust 区域和 DMZ 区域。这些区域分别代表了不同的安全级别，安全级别由高到低依次为 Local、Trust、DMZ、Untrust。Untrust 区域连接外部 Internet 网，Trust 区域连接云内网，DMZ 规划资源池用于业务需要的 WebServer，MailServer 及其他的需要暴露到公网的服务。

此处由于 DMZ 区域的资源需有云管理平台统一管理，故需要为管理网络同样配置虚拟防火墙实例，按照同样的方式配置 DMZ 区。即 Trust 域为云管理平台，DMZ 区连接资源的管理面网络交换机，此虚拟防火墙不提供公网到 DMZ 的访问能力。

3.1.3.2.3 多业务、多租户网络隔离

系统提供以下几个层次的网络隔离手段来达到端到端的多租户的业务安全

系统网络系统物理隔离

基础设施的云管理平台、云存储平台、云计算平台物理隔离

整个系统中网络按照通信类型分为管理、存储、业务 3 类，所有资源池中的计算资源（服务器）通过多网卡（6 个）连入不同的物理网络，提供完全的物

理隔离基础设施与公网之间通过防火墙隔离

所有基础架构的设备均通过防火墙与公网隔离，提供 DMZ 区来开放必须对外提供的服务的 Web,Mail 服务，通过内部的防火墙加强对核心的云管理平台、云存储平台、云计算平台网络进行保护

租户隔离

通过将不同租户的虚拟机网络使用不同 VLAN 来达到隔离互不影响

业务隔离

不同业务之间 VLAN 隔离

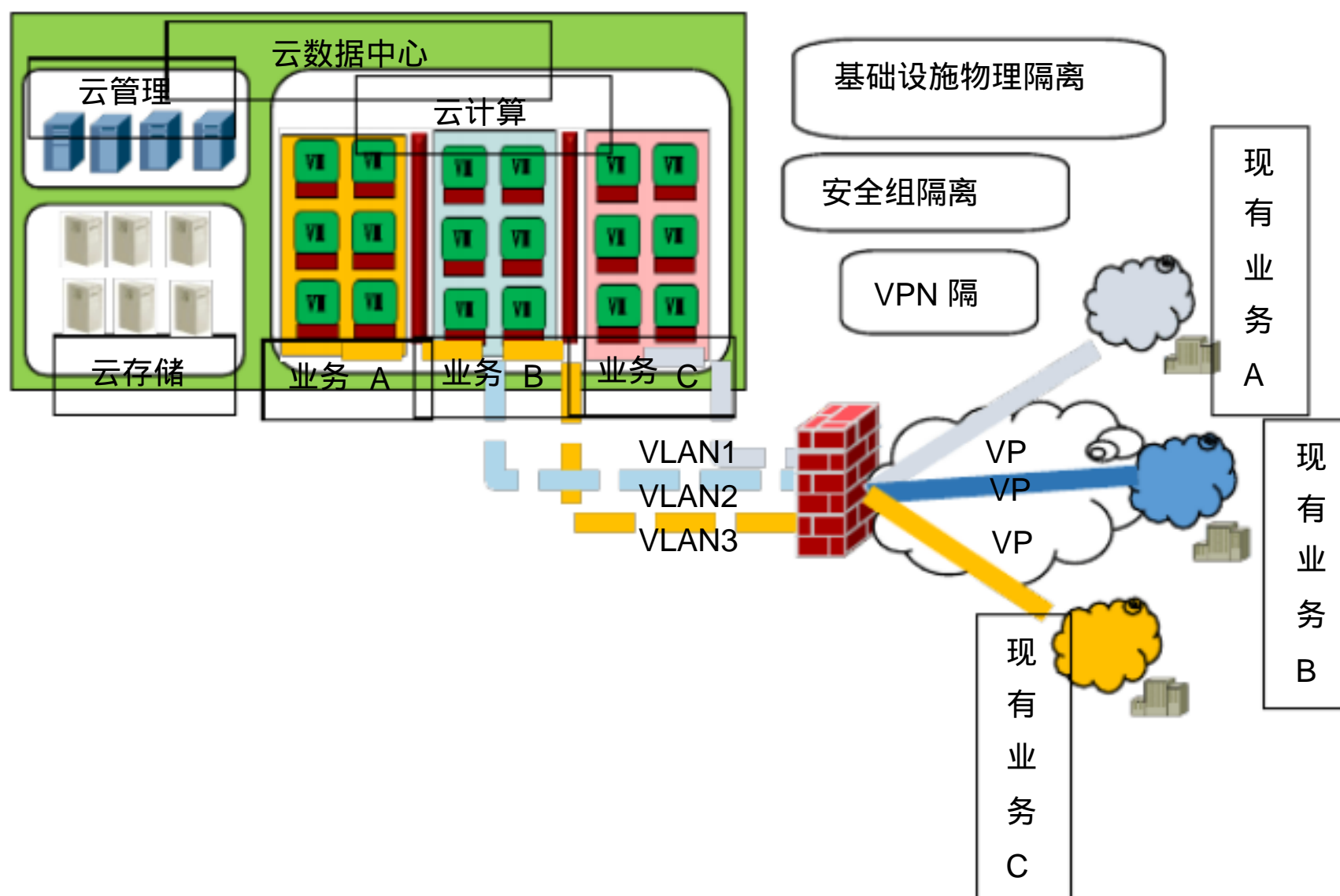
提供同一用户的不同业务和不同用户的业务均采用 VLAN 隔离来加强网络安全

业务之间 VPN 隔离

通过 VPN 来连接业务云和 MDCN 网络中同类型业务，达到整合业务系统的目的，同时保证也业务隔离互不影响

同一业务虚拟机之间安全组隔离

3.1.3.3 与其他系统对接情况



如上图所示，与已有的业务系统对接，完成统一的业务系统。实现上通过虚拟防火墙提供的 VPN 能力来连接业务云中的各网中业务和 DCN 中的业务。

虚拟防火墙是一个逻辑上的概念，每个虚拟防火墙都是 VPN 实例和安全实例的综合体，能够为虚拟防火墙用户提供私有的路由转发业务和安全服务。每个虚拟防火墙中可以包含三层接口、二层物理接口、二层 VLAN 子接口和二层 Trunk 接口 +VLAN。

VPN 实例与虚拟防火墙是一一对应的，它为虚拟防火墙提供相互隔离的 VPN 路由，与虚拟防火墙相关的信息主要包括：VPN 路由以及与 VPN 实例绑定的接口。VPN 路由将为转发来自与 VPN 实例绑定的接口的报文提供路由支持。

安全实例为虚拟防火墙提供相互隔离的安全服务，同样与虚拟防火墙一一对应。安全实例具备私有的 ACL 规则组和 NAT 地址池；安全实例能够为虚拟防火墙提供地址转换、包过滤、ASPF 和 NATALG 等私有的安全服务。

通过在 DCN 网络侧的防火墙，为不同的业务配置不同的 VPN 实例来达到业务隔离的目的。一方面是为了解决业务多实例的问题，更主要的是为了将一个物理防火墙划分为多个逻辑防火墙来用。多个逻辑防火墙可以分别配置单独不同的安全策略，同时默认情况下，不同的虚拟防火墙之间是默认隔离的。

3.1.4 部署架构设计

系统部署的架构如下图所示：

为了便于对资源分类和异构管理，以及对后续的扩展，每个数据中心均为独立的系统。每个数据中心都有自己的管理节点，提供各自的管理门户，各管理节点的用户中心指向主控管理节点的用户中心。其效果是同一套用户和权限可同时管理多个数据中心，并且在支持各类异构资源池的同时，能够保留该资源池的特性，当其中一个资源池中的管理节点发生故障时不会影响其他管理节点的正常运行。用户还可以为不同的数据中心指定资源池的密级，只有指定密级的资源才可以创建在这些数据中心内。

3.2 功能设计

本项目采用易讯通 ECloud 云管理平台对数据中心的计算资源、网络资源、存储资源进行统一的资源整合、资源管理、资源调度、运维管理。

用户可以通过统一的管理界面及可视化拓扑展示，轻松的构建自己的云平台。内置丰富的资源管理与流程配置功能，系统将原本需要手动分配的计算、网络、存储设施抽象为统一管理、易于调度、按需分配的资源；使用云平台系统可以把资源整合封装，对外提供按需分配、灵活使用的各类 IT 资源服务，满足资源和业务的管理。

3.2.1 异构资源管理

可实现对各种异构资源的统一管理，包含计算（EVC、vmware、xenserver、KVM 等）、存储、网络等。并对资源池中的实例进行生命周期管理（如虚拟机的创建、修改、回收、迁移、克隆等），实现对资源的统一管理和调度分配（如高可用、负载均衡等策略）。

3.2.2 用户管理

按照企业的需要，创建多种用户、角色和权限，并且配置授权、审计、安全等三员管理模式。提供方便的扩展接口，便于和其它用户认证系统进行集成。

3.2.3 监控告警

监控云平台中运行的各种资源、服务、及系统本身的性能数据和运行状态，进行容量管理、健康分析和告警管理，及时发现异常和潜在问题，基于数据对资源池、宿主机、虚拟机绘制网络拓扑图、做出容量趋势分析。

3.2.4 存储管理

云管理平台通过软件定义存储功能，实现分布式存储、磁盘阵列、存储设备的管理，为用户提供对象存储、弹性块存储、文件存储、网盘等服务，满足用户在使用虚拟主机时存储大量数据和文件的需求。

3.2.5 应用管理

方便管理员设计和发布多种类型的弹性应用服务，提供基础环境、商业软件、工具、数据分析等多类服务的生命周期管理（设计、发布、管理、监控、运维等），例如 Hadoop 环境、R 语言环境、Docker、CAD 软件、高性能计算服务等

3.2.6 流程管理

提供服务过程中所涉及的相关流程。其中包括接收服务请求中的业务申请、变更、终止等；此外，针对系统中出现的各类问题和事件，通过工单的方式进行处理流程跟踪。

3.2.7 资源调度管理

云管理平台自动收集各资源池中资源的使用情况，包括 CPU 使用率，内存使用率、可用存储空间等信息，用于判断资源的可用和容量情况。

管理员通过系统设置功能配置资源分配和调度的策略，如基于 CPU 或基于内存使用情况选择 Hypervisor，虚拟机使用填满或分散方式放置等。

当管理员创建资源或者上层运营管理平台接受用户的服务申请并下发资源创建命令时，资源管理平台会根据当前资源池的资源可用情况和设置的策略来合理分配和放置资源。

4 建设方案亮点

4.1 规模化的虚拟化数据中心

易讯通 ECloud 云管理平台具有管理大规模云数据中心的能力，通过管理集群可管理不低于 5,000 颗 CPU 不低于 50,000 台虚拟机的设备。

4.2 兼容异构的虚拟化

易讯通 ECloud 云管理平台支持多种虚拟化技术，通过单独建立的云平台管理系统，在保留原虚拟化技术特性的同时，提供了异构管理的能力，

4.3 灵活的管理方式

易讯通 ECloud 通过对多数据中心单独建立系统，接入主控管理的方式，实现了异地数据中心的统一管理。

4.4 可靠的安全保障

易讯通 ECloud 云管理平台给云环境提供了可靠的安全保障。主要体现在以下三个方面：

分权分域

ECloud 云管理平台对用户进行分权、分域的配置，对于不同的资源，平台可对用户设置不同的角色和权限，保证了云管理平台运维体系的安全、可靠。

多租户的资源隔离

ECloud 云管理平台支持多租户的配置，对于本次项目，可以将运行相同业务系统的资源配置在一个租户中，这样可以保证租户之间的计算、网络、存储资源相互隔离，互不影响。

用户数据安全

ECloud 云管理平台保证了用户数据的安全。当用户虚拟机或虚拟磁盘被销毁时，云平台可对用户数据进行安全擦出，保证了用户数据不泄露，加强了用户系统的安全性。

4.5 自动化的运维

易讯通 ECloud 云管理平台提供了先进的自动化运维手段，减少了管理员运维工量。

云管理平台支持动态的资源调度，保证云平台上所管理的物理服务器的资源使用率都保持在一个平稳的状态，避免了物理服务器使用率高低不均的情况。这样也降低了业务系统宕机的几率。

云管理平台通过在线迁移技术，同样支持虚拟机的高可用性。避免了因物理服务器宕机而引起的业务系统的中断，提高了上层业务系统的服务等级。

4.6 健壮的运维保障

易讯通 ECloud 云管理平台提供了健壮的运维保障，提供了高效、稳定的资源监控、计量功能，支持告警、日志、事件，以及多维度的统计报表，提高了运维人员的工作效率，也为运维人员提供了精确、可靠的云运维数据。