Inline Text Wrapping Picture

北京邮电大学

硕士研究生学位论文开题报告

学 号: 2017180219

姓 名: 孙志远

学 院: 软件学院

专业(领域): 软件工程

研究方向: 云计算与大数据

导师姓名: 崔毅东

攻 读 学 位: 工程硕士

2018年12月1日

|  |  |  |  |
| --- | --- | --- | --- |
| 论文题目 | 云安全服务平台的设计与实现 | | |
| 选题来源 | 其他 | 论文类型 | 应用研究 |
| 开题日期 | 2018-12-04 | 开题地点 | 北京邮电大学 |
| **一、立题依据（包括研究目的、意义、国内外研究现状和发展趋势，需结合科学研究发展趋势来论述科学意义；或结合国民经济和社会发展中迫切需要解决的关键科技问题来论述其应用前景。附主要参考文献目录）（不少于800字）**  随着计算能力的指数级增长和各种计算设备的爆炸式应用，IT基础设施正在发生深刻的变化，虚拟化技术、软件定义网络、移动互联网技术逐渐从概念走向实际应用，云计算的兴起，BYOD的普及改变了传统的数据中心架构，而分布式云计算逐渐成为了主流的架构模型。  服务的普及和观念的更新使云计算得到了广泛的认可与接受，一大批云计算服务提供商也涌现了出来，包括知名的Amazon AWS、Google GCE以及Microsoft Azure。同时，国内也出现了像阿里云、腾讯云、移动云等一批优秀的云服务提供商。越来越多的企业往云上聚集，越来越多的应用和系统也被部署在云上。  然而，大规模应用在云端集中，使得传统的安全问题都随之迁移到了云上，新的技术也同时带来了新的安全问题。云计算的兴起，使得传统的网络边界变得模糊甚至消失，这给传统的防护思想和安全产品带来了巨大的挑战。与此同时，非法利用和破坏信息系统也发展成为了有组织的犯罪行为和敌对国家的活动。网络攻击的实施者已经不再是个人，而是有着明确的政治、经济利益目的的“黑产”组织。网络空间的威胁已经呈现出集团化、工具化、流程化、规模化的趋势，应用系统面临着比过去更加严峻的安全考验。  事实表明，新型的安全问题也必须由新型的技术手段来进行应对！云的出现使得All as a Service成为了可能，Security as a Service作为安全服务的一种，也慢慢全面和强大起来。它传承于传统安全但是却比传统安全服务更加全面、更加强大。借助于云端的计算能力，不仅可以采用机器学习、人工智能等新技术、新方法来主动抵御安全威胁而且颠覆了传统的安全服务方式，使得安全能力更加多样化、更具有针对性并且获取安全能力的成本更加低廉、服务的配置和使用变得更加简单便捷。  那么具体到安全即服务来讲，目前的云服务提供商和用户各自的安全职责和安全需求是什么？现阶段云服务平台采用了什么样的方式提供服务？什么样的云服务平台更加合理，能够更高效满足现阶段的安全需求？这些都是值得研究和探讨的问题。这篇论文从企业用户安全需求和工程实际的角度出发，结合当前技术、框架，分析和设计一个专注于提供安全服务的云安全服务平台。  参考文献：  [1]李志勇,李蒙,周悦.大数据时代云安全[M].北京:化学工业出版社,2016.  [2]胡志昂.信息系统等级保护安全建设技术方案设计实现与应用[M].北京:电子工业出版社,2010.  [3]刘焱.基于开源软件打造企业网络安全[M].北京:机械工业出版社,2018.  [4]董超,胡炽维.Spring Cloud微服务架构开发实战[M].北京:机械工业出版社,2018.  [5]陆平.基于Kubernetes的容器云平台实战[M].北京:机械工业出版社,2018.  [6]叶龙胜.基于Docker容器的SaaS模式云应用平台的研究与设计[D].北京:北京邮电大学,2017.  [7]彭荣.SaaS模式下，多租户系统架构及关键技术研究[D].大连:大连海事大学,2010.  [8]许慧.基于Zabbix的云监控系统的设计与实现[D].北京交通大学,2018.  [9]徐全才.基于多租户重要度SaaS系统服务质量提升的研究与实践[D].北京:北京邮电大学,2017.  [10]周荃.云计算资源管理中QoS保障机制研究[D].北京:北京交通大学,2013.  [11]丁滟,王怀明.可信云服务[J].计算机学报，2015.  [12]赵少卡,李立耀.基于OpenStack的清华云平台构建与调度方案设计[J].计算机应用,2013.  [13]M.Usha,J.Akilandeswari,A.S.Syed Fiaz.An efficient QoS framework for Cloud Brokerage Services[C].2012 International Symposium on Cloud and Services computing,2012.  [14]Mahmud Hossain. Jugo:A Generic Architecture for Composite Cloud as a Service[C].2016 IEEE 9th International conference on Cloud Computing,2016.  [15]Christian Baun, Marcel Kunze, Viktor Mauch.The KOALA Cloud Manager:Cloud Service Management the Easy Way[C].2011 IEEE 4th International Conference on Cloud Computing,2011. | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **二、研究内容和目标（说明课题的具体研究内容，研究目标和效果，以及拟解决的关键科学问题。此部分为重点阐述内容）（不少于2500字）**  一、研究的内容主要包括以下几个方面：  1、新型的安全威胁，特别是云计算兴起带来的新的安全风险：随着技术的发展和时代的进步，出现了很多新型的安全威胁比传统的安全威胁更具有杀伤力。传统威胁包括恶意代码，包括病毒、僵尸网络、木马、蠕虫，此外还有后门、下载器、间谍软件、内核套件、勒索软件等其他类型；相应的解决方案基于边界、规则、监测。如防火墙、黑白名单、IPS/IDS。常见的防御体系有：边界防御体系，UTM、WAF、FireWall都是这一体系的产物；纵深防御体系，在多层部署防御措施，如数据库端、服务器端、网络层、网络边界、甚至包括服务器内核级别的检测与对抗。  新型的安全威胁有由于基础软件的改进以及业务系统的改进而产生的进化版DDoS攻击、APT等，相应的新型的安全解决方案出现包括：新型的安全解决方案基于感知、预防、自动智能化。如网络安全态势感知、威胁情报、动态黑白名单、安全信誉服务以及利用安全大数据和机器学习来进行安全数据抽取、收集、分析、建模从而进行智能识别，智能防护等。新型的防御体系代表为塔防体系，是纵深防御的加强，它突破了传统基于边界防护的设计理念，从网络、主机、数据库层面，依托人工智能技术以及沙箱技术，结合威胁情报提供全方位的Web纵深防护。具有自我防御能力，并具有云的管控能力和威胁情报数据。  2、目前国内外SaaS平台的现状、云服务用户和Saas云服务提供商对于安全的需求现状：云计算正在改变以往的服务模式和用户思维，许多服务不管是硬件(IaaS)，还是平台(PaaS)亦或者是服务(SaaS)都能一键获取和接入。因此，云计算和服务真在彰显出越来越大的价值，其内涵和内容也在急速丰富的过程中，产品和解决方案琳琅满目，从云计算的基础服务到安全服务再到人工智能、物联网、大数据。而且云计算服务提供商也涌现了很多家，其中包括国外知名的Amazon AWS、Google GCE以及Microsoft Azure;国内的阿里云、腾讯云、移动云等。具体到安全服务有主机安全、网络安全、业务安全、应用安全、数据安全、安全管理等各个方面层次的服务。云计算时代下，整体的IT基础架构发生了根本性的变化，信息安全的防护，越来越多地需要用户（云租户）密切参与，即整体的安全责任是由云租户和云服务商共担。“谁分担得多，谁分担得少”主要随着所采取的服务模式（SaaS、PaaS和IaaS）的不同而不同。  （1）SaaS：应用软件层的安全措施由客户和云服务商分担，其他安全措施由云服务商实施；  （2）PaaS：软件平台层的安全措施由客户和云服务商分担。客户负责自己开发和部署的应用及其运行环境的安全，其他安全措施由云服务商实施；  （3）IaaS：虚拟化计算资源层的安全措施由客户和云服务商分担。客户负责自己部署的操作系统、运行环境和应用安全。云服务商负责虚拟机监视器（Hypervisor）及底层资源的安全。  3、云平台的架构理论：常用的虚拟化技术、容器技术，如OpenStack、Docker和Kubernetes；虚拟化技术和容器技术是近年来很流行的技术，虚拟化技术充分利用了计算资源使得同一台机器可以运行多个虚拟机提供多个服务，而容器技术提供了更加轻量化的打包运行方式，为微服务提供了很好的容器。Kubernetes是Docker容器的编排者和管理者来进行负载均衡、工作调度、维护高可用性。对于虚拟层的研究对于平台的整体安全很重要 ，IaaS层作为基础层与PaaS、SaaS这些都是相辅相成的，基础架构完备性和安全性直接决定了上层平台甚至整个服务系统的性能和稳定性。  4、云平台业务系统端的设计，包括服务端系统以及管理端系统的设计：最重要的部分是平台的功能模块的设计，这里分为两部分：首先，平台的服务端如何设计，即用户如何通过平台获取安全服务，如何配置和管理安全服务，安全情况详情如何展示给用户以及如何生成安全服务报告等内容，由于用户并没有专业的安全知识，所以客户端的操作流程要明了，配置过程要简单，尽量符合用户使用逻辑。在展示方面要层次分明并且一目了然，尽量契合用户的关注点。然后，管理端应该如何设计，其中包括如何进行安全服务的配置，如何管理用户，如何进行平台的监控和运维等问题。管理端需要能够监测到管理端自身的安全情况，客户的服务情况以及平台的运行情况，需要做到和服务端互通有无，全局统筹。  （1）角色分析：云安全服务平台的涉及到了安全服务的需求方即用户以及安全服务的提供方即平台方，其中平台方主要的角色是运营管理人员。所以角色主要分为用户以及运营管理人员。  （2）功能列表：   |  |  |  |  | | --- | --- | --- | --- | | 系统 | 模块 | 功能 | 功能描述 | | 服务端 | 身份认证 | 注册 | 用户注册云安全服务平台 | | 登录 | 用户登录到云安全服务平台控制台 | | 安全服务 | 申请安全服务 | 用户根据平台的安全能力进行安全服务能力组合并申请使用安全能力 | | 配置安全服务 | 在安全服务审核通过后，需要通过配置服务才能作用到保护目标 | | 查看安全服务报告 | 根据配置可以手动或者自动生成安全服务报告 | | 查看安全服务详情 | 可以通过详情面板查看安全服务的详细情况，不同的安全能力展示的安全信息不同 | | 管理 | 资产信息 | 用户可以管理添加到平台的资产的信息 | | 个人信息 | 用户可以管理个人的信息 | | 管理端 | 认证 | 身份认证 | 认证管理员的合法身份 | | 权限认证 | 认证管理员拥有的权限 | | 平台运营管理 | 用户管理 | 对平台上的用户进行管理 | | 服务管理 | 对平台接入的服务进行管理 | | 监控管理 | 对平台的资源和性能进行监控 | | 配置管理 | 对平台自身以及相关的服务进行配置 |   表1 功能列表  （3）用例图：图1为平台的用例图,其中：  用户的用例包括：登录，注册平台、申请安全服务、配置安全服务、查看安全服务报告以及查看安全服务详情等。  运营管理人员的用例包括：身份，权限认证、用户管理、服务管理以及平台监控，平台监控包括平台安全监控和平台的资源性能监控等。  图1 平台用例图  （4）功能模块图：图2为该平台的功能模块图：  服务端包括2个子系统7个模块，分别门户系统的登录、注册模块和控制台系统的个人中心管理模块、资产管理模块、安全服务模块、服务配置模块和报告管理模块。  运营端包括4个模块分别是用户管理模块、服务管理模块、监控管理模块以及配置管理模块。  TIM截图20181213201005  图2 云安全平台功能模块图  （5）系统平台层次架构图：图3为系统平台的层次架构图，共分为3层。  第一层：最下层的基础层，即IaaS，如果是公有云，一般由云服务提供商提供；如果是私有云，则由企业或者个人自行提供，通常是以虚拟化的方式搭建。它为整个平台提供了最基本的运行环境。包括基本的计算资源、网络资源和存储资源。  第二层：中间层为平台层，即PaaS，提供一些基础服务和通用的服务，如数据服务和文件服务等，这些基础通用服务是上层服务必须的元素，它为业务层提供了稳定的运行环境和必备的支撑服务。  第三层：最上层为业务层，业务层提供专业的服务，如安全能力服务以及Web服务和一些支撑服务，如认证服务、加密服务、调度服务和监控服务等。在这一层中，为了更好地充分利用资源，最大化效能。可以采取容器技术将各个服务封装起来，统一管理，统一调度。从而形成一个整体服务池，对外按需提供服务。  当有业务请求时，先通过统一的API网关进行调度，然后到注册中心去找合适的服务，经过负载均衡服务来统一分发到可用的后端服务进行处理返回给用户。    图 3 系统平台层次架构图  5、其他相关知识，如SpringCloud、安全认证、数据的加密解密、数据安全传输与存储、任务调度、性能监测等：  （1）SpringCloud：容器为微服务的发展奠定了基础，通过研究SpingCloud以及相关的微服务的架构方式可以得到一个具有拓展性伸缩性和高可用性的系统；  （2）安全认证：安全认证是要在系统的入口把控安全，通过对访问者的身份核查，属性验证和权限鉴定可以保证平台系统内部的安全；  （3）数据的加密解密：客户可选择把数据加密后再上传到云计算平台,加密密钥由用户自行管理;也可用云服务商的密钥管理服务或其提供的硬件加密设备加密数据,但此种方式对大规模处理不适用,还需客户自己实现加解密过程。选择服务端加密时客户需用云服务商提供的客户端开发API。客户有时希望数据保存在磁盘时加密,在内存中处理时不加密，以尽可能不用更改已有的应用的程序,即实现数据的透明加密。  （4）对数据的交换、转移与分享,主流云计算解决方案都支持标准的加密传输协议,有利于云平台与外界及系统间进行敏感数据传输的要求。为保证数据传输安全。  （5）由于向用户提供安全服务是一个动态的过程，所以会涉及到任务的调度；  （6）由于管理端要监控整个平台的负载状态和资源使用情况，所以需要采取合理的方式对系统的基本参数进行监控。  二、研究目标  研究目标是设计一个实用的，符合实际需求的云安全服务平台，此处的安全有3层含义：  1、 对用户提供安全服务，这是云平台的价值所在。通过SaaS平台，可以为用户提供各种各样的服务，其中也包各种安全服务，即Security as a Service。传统的安全能力的获取时通过购买安全软件自行部署到用户业务系统，但是通过安全能力服务平台，可以实现一键接入，按需开通，按量付费。简单便捷而且还可以选择搭配不同的安全能力组合来进行针对性防护，真正做到投入很少的人力和费用就能从云端架构纵深防御体系，实现自助选取，自助管理以及自助生成安全报告。即对于用户需要做到：  （1）安全能力自由组合  （2）按需开通  （3）用户自助管理  （4）安全详情展示与报表生成  2、 云平台本身是安全的，这是云平台的服务基础。云平台要提供对外安全服务的基础是保证自身系统足够安全，这种安全应该是从内到外的。根据国家网络安全法等级保护工作的推进，将原来单纯的信息系统拓展到了很多个领域，其中包括云计算领域、移动互联领域、物联网领域、工控领域和大数据领域，其中首先强调的就是云等保，对于云服务系统的要求将从技术安全（物理和环境安全、网络与通信安全、设备与计算安全、应用与数据安全）到管理安全（管理策略和管理制度、管理机构和人员、安全建设管理、安全运维管理）双管齐下。具体到安全服务云平台，首先应该做到使用安全的架构，能够抵御外来无意攻击，使用安全的认证和入侵检测服务，来抵御有意的侵入。即服务系统自身需要满足：  （1）安全的架构  （2） 基础防护能力  （3）安全的认证  3、用户信任平台是安全的，这是用户合作的重点。在做到安全系统提供安全服务之后，我们还需要让保证用户的服务质量有保障，这样才能做到全面的安全，其中最重要的是保护用户数据的安全。具体来讲，特别是安全漏洞这类敏感的数据，应该做到数据的加密存储和传输，防止数据的泄露。即可信服务应该做到：  （1）QoS服务质量保证  （2）数据防泄漏和丢失 |

|  |
| --- |
| **三、研究方案设计及可行性分析（包括：研究方法，技术路线，理论分析、计算、实验方法和步骤及其可行性等）（不少于800字）**  研究方法采取：  分阶段进行研究，分层进行设计，逐要素进行试验验证，最后进行整合，即从需求分析到应用设计、从理论基础到技术选型、从底层到应用层、从模拟到验证。重要模块的分析应该结合相关文献、已有系统和工程实际进行深度分析，必要时要经过相关实验和操作的验证。  研究路线如下：  1.首先要进行需求调研，特别是SaaS安全服务用户的需求，然后形成需求分析报告。  2.接着对虚拟化技术、容器技术和容器编排系统的原理和工作方式进行研究，这里需要注意总结和对比不同技术之间的差别，同时对于Kubernetes这种比较复杂的系统来说，要清楚它的运作流程，组件之间的关系以及重要组件的内部作用流程。对于这些比较抽象的工具，应该进行实际配置和运行，对其功能和性能进行评估，生成评估报告。  3.然后对目前的SaaS平台的架构进行研究，重点分析其自身的安全性和提供安全服务的方式。思考云安全平台的架构设计。  4.从底层开始进行层次模块设计，并且对重点模块进行模拟，验证可行性。对不可行的设计进行调整和重新设计。设计包括平台的层级结构、每个子系统的功能和子系统之间的交互关系、每个子系统的关键组件以及工作的主要流程以及必要的支撑服务，如安全认证、安全加密、任务调度、系统监控等系统所需的模块。此外还包括业务系统端的功能模块，用户用例，使用流程等相关的设计。最后输出概要设计报告和技术平台选型报告。  5.最进行整合设计，进行集成验证。经过调整和优化达到要求后输出详细设计报告，接着进入实现阶段。  6.在实现阶段首先要确保有可用的环境和实验资源，然后配置好所需的实验环境，包括基础的云环境和开发环境  7.在开发过程中需要进行单元测试和集成测试，及时记录发生的问题和遇到的瓶颈，开发完成之后将系统部署到云端，经过相关配置后以云Web防火墙为例，展示系统如何通过安全服务云平台使用安全防护能力保护用户的Web应用以及用户如何使用系统来配置和管理服务、查看服务展示信息和生成安全服务报告以及如何通过管理端系统对整个系统进行配置、管理和监控等一系列功能，最后生成测试报告。 |

|  |
| --- |
| **四、本研究课题可能的创新之处（不少于500字）**  1.该课题涉及到了对新型威胁和对新型安全能力的研究，特别是云安全相关的安全威胁：“云安全”是指对云平台自身的安全保护，主要利用面向云架构/环境的安全策略、技术产品，解决云环境下的安全问题，提升云平台自身的安全性，保障云计算业务的可用性、数据机密性和完整性、隐私权的保护等。  2.该课题涉及到了虚拟化技术的研究，包括虚拟机和容器技术，特别是Docker和Kubernetes是比较新的技术，通过这些技术可以实现服务更快很更地实现和交付：借助Docker的容器能力和Kubernetes的编排功能，可以构建多个安全能力服务集群，并实现跨集群调度。综合其他技术、框架形成完整、健壮的云安全平台解决方案。  3.该课题涉及到了服务质量的研究，目前云平台发展迅速，但是用户却有很多顾虑，其中包括云服务的稳定性，安全性等服务质量的不确定性以及数据存储在三方服务公司的风险性。如何在云服务中确保服务质量也是一个很值得探讨的问题，具体到本次课题，研究了在提供安全服务时云平台应该注意的服务质量问题。  4.该课题涉及到了平台的设计。从产品的角度，从用户的使用场景和使用流程出发思考如何去设计系统能够有更高的易用性，使系统对用户更加友好；如何能够更加满足用户的功能需求，使每一项功能点贴近用户的关注。 |
| **五、研究基础与工作条件（1.与本项目相关的研究工作积累基础 2.包括已具备的实验条件，尚缺少的实验条件和拟解决途径）（不少于500字）**  理论基础：  1、目前安全公司提供的安全服务产品：  杀毒软件：如360杀毒，金山杀毒，腾讯电脑管家等；抗DDoS攻击：如电信云堤；WAF防火墙：如开源OpenResty；Web漏洞扫描；API网关：如API网关Kong；风险控制系统：如开源风控系统Nebula；数据库审计；主机加固：阿里云“安骑士”；代码审计：如RIPS和VCG；网络入侵检测；主机入侵检测；数据防泄漏系统；统一威胁管理平台；流量审计；数据库防火墙；VPN：如开源OpenVPN；反垃圾邮件；威胁情报；移动应用加固；蜜罐与攻击欺骗；RASP应用实时防护：如开源OpenRASP；态势感知系统；智能反欺诈；云防火墙；安全管理中心：如开源软件OSSIM、OpenSOC以及Apache Metron等。  2、SaaS平台，特别是安全服务目前的发展状况：  在云计算时代，越来越多的企业将其业务迁移到云端，并云端运营其业务或者进行数据灾备存储等。IT基础资源集中化的趋势，以及客户的不断上云，将会使得云安全的变得愈来愈重要。如果云平台的安全等级以及防护出现问题，其结果将会是致命的。因为，我们看到，主流的云计算厂商及供应商，均在云安全领域进行了巨大的投入和产品升级，以应对云计算时代带来爆发的云安全需求。随着越来越多的企业往云上聚集，云服务提供商对云上业务、数据的安全所肩负的责任担子越来越重，势必会对安全问题更加谨慎，将与专业的云安全提供商进行更密切的合作，所以来自云服务提供商的安全需求将进一步释放；另一方面，正如第一节中所提及的那样，云上的安全责任是云服务提供商与租户共担的，所以企业级客户对云安全的需求也将持续增加。  全球云安全市场主要由四种参与者组成：云平台服务提供商（如阿里云、腾讯云、金山云、亚马逊AWS、Salesforce等）；专业的云安全解决方案提供商（往往值云安全初创公司，如Zscaler、Symplified、安全狗、云锁等）；传统IT安全解决方案提供商（如趋势科技、赛门铁克、迈克菲、360等）；大型IT厂商（IBM、惠普、英特尔等）。云平台服务提供商在云安全领域中的分工比较特殊。下面具体以阿里云和腾讯云为例，说明云平台服务提供商在云安全领域所扮演的角色。云上的安全有明确的责任划分，并且随租户所采取的云服务模式（IaaS、PaaS、SaaS）的不同而不同。  阿里云作为国内知名的IaaS云平台服务提供商，它所采取的风险共担模式具有代表性，可说明众多IaaS提供商的一般情况——即阿里云负责云基础设施层面的安全，用户则要对自己的虚拟化层以上负责。在虚拟化层，阿里云同时提供云盾以及通过引入第三方生态合作伙伴的方式来提供安全服务，这种安全责任共担模式最终的目的是帮助用户减轻安全运营负担，更专注于核心业务。  腾讯云与阿里云的安全责任划分大致相同，主要差别在于其提供的云安全产品所覆盖的领域上的不同。其安全防护可分为三个方面：云基础设施安全、云租户安全、业务安全。其中腾讯云安全团队的工作重点是对基础设施的保障；云租户安全和业务安全一部分自己做，仅提供标准化安全服务，另一部分开放给技术合作伙伴，来给不同行业的客户提供定制化的安全服务。而这里的合作伙伴就是专业的云安全解决方案提供商和传统的IT安全解决方案提供商还有IT大厂，能够进行安全能力的整合和集成。  3、OpenStack的架构以及相关组件的工作方式  OpenStack是一个通过一定的虚拟方式将计算资源，存储资源、网络资源进行池化并实施统一管理的云操作系统，目前具有20多个模块，其中核心模块有：  （1）Nova管理计算资源，VM的生命周期  （2）Neutron管理网络资源，提供网络连接服务，负责创建和管理L2,L3网络，为VM提供虚拟网络和物理网络连接  （3）Glance为VM提供OS镜像，管理VM的启动镜像，Nova创建VM时将使用Glance提供的镜像  （4）Cinder提供块存储，为VM提供块儿存储服务。cinder提供的每一个Volume在VM看来类似于一块虚拟硬盘，一般用做数据盘  （5）Keystone提供认证服务和权限管理服务  （6）Horizon提供操作界面  另外还有其他服务如：  （1）Swift提供对象存储，VM通过RESTful API存放对象数据  （2）Ceilometer提供监控服务，计量服务，为报警，统计或者计费提供数据  4、Docker的实现原理以及工作方式  Docker以容器技术为核心的一套应用的构建，分发，执行的体系和生态。其生态完整包括：  1.Docker Engine Docker容器的管理，包括容器的创建，销毁  2.Docker Hub 镜像仓库  3.Docker Machine Docker虚拟机  4.Docker Swarm 集群管理工具，其主要作用是把若干台Docker主机抽象为一个整体，并且通  过一个入口统一管理这些Docker主机上的各种Docker资源  5.Docker Component  5、Kubernates容器编排的架构以及相关组件的工作方式  Kubernetes（k8s）是自动化容器操作的开源平台，这些操作包括部署，调度和节点集群间扩展。Kubernetes不仅仅支持Docker，还支持Rocket。Kubernetes的核心概念如下：  （1）Pod：Pod是Kubernetes的基本调度单元，一个Pod包含一个或者多个容器，Pod中的容器都部署在同一台主机上，并且共享资源。  （2）Replication Controller:Replication Controller用户管理、控制Pod的副本数，用于解决Pod的扩容、缩容问题。通常，分布式应用为了性能或者高可用性，通过负载实现动态的收缩，这里由Controller来保证这些性能。  （3）Service：Service是真实应用服务的抽象，定义了Pod的逻辑集合和访问这个集合的策略，Service的引入旨在保证Pod的动态变化对访问端透明，访问端只需要知道Service的地址，由Service来提供代理服务。  （4）Label：Kubernetes中使用Label来标识任意的API对象，供其他对象进行查找。  （5）Node：Node也称为Worker或Minion节点，是主从架构集群的计算单元，是分配给Pod的宿主机。  （6）Master:Master节点时Kubernetes的分布式集群管理控制中枢，所有的任务都通过这里进行统一分配。  6、SpringCloud微服务的架构以及相关组件的工作方式  springCloud是基于SpringBoot的一整套实现微服务的框架。他提供了微服务开发所需的配置管理、服务发现、断路器、智能路由、微代理、控制总线、全局锁、决策竞选、分布式会话和集群状态管理等组件，其中核心的模块包括：  （1）Zuul：API网关，外部或者内部的非Spring Cloud项目都统一通过API网关（Zuul）来访问内部服务。  （2）Eureka：服务注册中心，所有的服务都必须要注册到Eureka网关接收到请求后，从注册中心获取可用服务。  （3）Ribbon: 负载均衡服务，请求由Ribbon进行均衡负载后，分发到后端的具体实例。  （4）Feign：通信服务，微服务之间通过Feign进行通信处理业务。  （5）Hystri：断路器，Hystrix负责处理服务超时熔断。  （6）Turbine：监控服务，Turbine监控服务间的调用和熔断相关指标。  其他：  1、性能监控系统Zabbix的原理和应用  2、安全认证的原理和应用  3、分布式任务调度系统的原理和应用  4、加密传输和加密存储的原理和应用  5、等级保护1.0与2.0的相关理论知识  开发语言、开发工具：  Java，Python以及相关工具如IntelliJ IDEA、JetBrains、PostMan、 Maven、Xshell、Xftp等  硬件基础：  个人的服务器和公司的服务器可以用来开发部署和测试软件系统  其他：  域名、开源软件、公司的设计团队和开发团队的支持 |

**学位论文工作计划**

|  |  |  |
| --- | --- | --- |
| 时间 | 研究内容 | 预期效果 |
| 2018.12.04-2019.01.04 | 课题调研 | 调研报告 |
| 2019.01.04-2019.02.04 | 需求分析 | 需求分析说明书 |
| 2019.02.04-2019.03.04 | 概要设计 | 概要设计报告 |
| 2019.03.04-2019.04.04 | 详细设计 | 详细设计报告 |
| 2019.04.04-2019.07.04 | 系统实现 | 可运行的软件系统 |
| 2019.07.04-2019.08.04 | 部署测试阶段 | 测试报告、缺陷总结报告 |
| 2019.08.04-2019.09.04 | 论文初稿 | 论文初稿 |
| 2019.09.04-2020.01.04 | 系统优化，论文修改 | 系统可稳定运行，论文可审 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 评  定  小  组  成  员 | 姓 名 | 职 称 | 单位名称 | 职务 |
| 漆涛 | 教授 | 北京邮电大学 | 成员 |
| 金跃辉 | 教授 | 北京邮电大学 | 成员 |
| 雷友珣 | 副教授 | 北京邮电大学 | 成员 |
| 崔毅东 | 副教授 | 北京邮电大学 | 成员 |
| 黄小红 | 副教授 | 北京邮电大学 | 成员 |
|  |  |  |  |
| 导师意见： | | | | |
| 选题来源于科研项目，研究内容合理，技术方案可行。  同意开题。 | | | | |
| 导师（签名）：  日期： 年 月 日 | | | | |
| 开题报告小组意见： | | | | |
| 组长（签名）：  日期： 年 月 日 | | | | |
| 学院意见（签章）： | | | | |
| 负责人：  日期： 年 月 日 | | | | |