河南开放大学2025年河南教师网络学院平台云服务项目

项目编号：豫财单一采购-2024-143

合同

甲方：河南开放大学

乙方：联通数字科技有限公司河南省分公司

河南开放大学2025年河南教师网络学院平台云服务项目合同

项目编号：豫财单一采购-2024-143

甲方：河南开放大学（以下简称甲方）

通讯地址：郑州市郑东新区龙子湖北路36号

邮编：450046

乙方：联通数字科技有限公司河南省分公司（以下简称乙方）

通讯地址：郑州市金水区北环路40号院1号楼

邮编：450000

第一条　合同标的物

乙方按本合同约定及甲方要求提供河南开放大学2025年河南教师网络学院平台云服务。该平台具有教师教育信息发布、培养培训、统计分析、多向互动、需求调查、课程资源服务等功能，具体服务内容（含课程资源服务）详见附件一（下同）。

1.1合同价款总额（含税）为：人民币￥1279000元（大写：壹佰贰拾柒万玖仟元）。（税率6%，合同不含税金额为：人民币￥1206603.77元（大写：壹佰贰拾万零陆仟陆佰零叁元柒角柒分），税额￥72396.23元（大写：柒万贰仟叁佰玖拾陆元贰角叁分）。）

1.2除本合同明确约定外，甲方无需另向乙方支付任何费用。

第二条　甲方权利和义务

2.1.甲方应向乙方提交执行本服务条款的联系人和管理甲方网络及云平台上各类服务的人员名单和联系方式；如以上人员发生变动，甲方应自行将变动后的信息通知乙方进行更新。

2.2.甲方对自己存放在乙方云平台上的数据以及进入和管理乙方云平台上各类产品与服务的口令、密码的完整性和保密性负责；因甲方原因致使上述数据、口令、密码等丢失或泄漏所引起的一切损失和后果均由甲方自行承担。

2.3.甲方进一步承诺：

2.3.1.甲方不会利用乙方提供的产品及/或服务散发含反动、色情等有害信息的电子邮件；

2.3.2.甲方不会将乙方所提供的服务用作非法代理服务器（Proxy）；

2.3.3.甲方不会利用乙方提供的产品及/或服务从事DDoS防护、DNS防护等经营性活动；

2.3.4.甲方不会利用乙方提供的资源和服务上传（Upload）、下载（download）、储存、发布如下信息或者内容，不会恶意为他人发布该等信息提供便利（包括设置URL、BANNER链接等）：

（1）违反国家规定的政治宣传和/或新闻信息；

（2）涉及国家秘密和/或安全的信息；

（3）封建迷信和/或淫秽、色情、下流、暴力、恐怖的信息或教唆犯罪的信息；

（4）博彩有奖、赌博游戏、“私服”、“外挂”等非法互联网出版活动；

2.3.5.甲方不会恶意破坏或试图破坏乙方网络安全，包括钓鱼，黑客，网络诈骗，通过虚拟服务器对其他网站、服务器进行攻击行为如扫描、嗅探、ARP欺骗、DDoS等。

2.3.6.甲方不得在乙方服务或平台之上安装、使用盗版软件；乙方有权拒绝使用盗版软件的相关应用系统在乙方服务或平台之上部署。

2.4.中华人民共和国的国家秘密受法律保护，甲方有保守中华人民共和国的国家秘密的义务；甲方使用乙方服务应遵守相关保密法律法规的要求，并不得危害中华人民共和国国家秘密的安全。

2.5.如果第三方机构或个人对甲方提出质疑或投诉，乙方将及时

通知甲方，甲方应及时解决相关事宜。

2.6 甲方有权对乙方的服务行为进行监督和检查。甲方对其认为乙方服务不合理部分有权要求乙方限期整改，乙方未按甲方要求整改的，甲方有权委托第三方处理，全部费用由乙方承担。

第三条 乙方权利和义务

3.1 乙方保证按合同约定及甲方要求提供安全评估服务，乙方应配备专业技术人员依照本协议约定及甲方要求向甲方提供云服务和售后支持等服务。本合同签订后3日内，乙方将指定负责人及专业人员的人员名单及联系方式以书面形式告知甲方。

3.2 乙方负责按合同约定及甲方要求完成本合同系统部署 并对云服务提供运营维护，乙方应当保证自身的网络、设备的安全性、稳定性，如发生以下情况，乙方应及时解决并避免对云服务产生影响：

(1)乙方网络出现问题，包括但不限于超负荷等；

(2)乙方自有设备或乙方使用的第三方设备出现故障；

(3)乙方自行拆离设备或通过其他方式导致网络中断；

(4)其他非因甲方原因导致的任何故障、网络中断等。

3.3 乙方有责任对提供云服务过程中发现的隐患及缺陷向甲方以书面形式提出，并按甲方要求进行及时处理，确保甲方系统、数据安全。

3.4乙方负责操作系统以下的底层部分及乙方提供的软件的运营维护，例如：云服务器、云数据库的相关技术架构及操作系统等。操作系统之上的部分（如甲方在系统上安装的应用程序）由乙方负责。

3.5 未经甲方书面同意，乙方不得将服务的全部或部分转由第三人承担，否则甲方有权直接解除本合同。

3.6乙方不得擅自暂停服务，如因系统调试、维护或升级等需要

而暂停云服务，需提前30日告知甲方并征得甲方书面同意。

3.7 如因乙方人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任。

第四条　付费方式

4.1 服务内容及明细（含课程资源服务）（见附件一）。

4.2 甲方应按约定的缴费方式向乙方缴纳服务费，甲方确认订单后，24小时内由乙方为甲方开通服务（包括完成系统部署等）。

4.3 自合同签订后，乙方完成云服务部署，乙方向甲方提供云服务服务方案、服务承诺，经甲方初步验收合格后，乙方提供付款的相关手续资料并开具发票后，甲方向乙方支付合同总价款的80%，即人民币1023200元；在本合同服务期最后一个月内，乙方提供云服务相关验收材料，甲方组织验收专家进行验收审核，最终全部验收合格后，甲方向乙方支付合同总价款的20%，即人民币255800元。

4.4 发票种类：

（1）乙方提供发票种类如下：

【 】增值税专用发票；　　【√】增值税普通发票；　　【 】服务业发票；【 】税局代开发票；　【 】其他发票：_____。

（2）本项目提供的发票应按照本合同约定内容，乙方根据服务的不同区别开具。

（3）如乙方开具发票不符合有关规定或存在异常，乙方承担由此导致的全部损失，包含但不限于甲方税费损失、滞纳金、罚款及其他相关损失。

4.5 银行信息：

合同乙方：　联通数字科技有限公司河南省分公司

开户名称： 联通数字科技有限公司河南省分公司

开 户 行： 中国工商银行股份有限公司郑州行政区支行

帐　　号： 1702029119201085202

4.6如在合同期内因资费政策调整,本合同中所述资费发生变动,经双方协商并签署书面补充协议后，双方按照新的资费标准执行。

第五条　质量保障和故障处理

5.1乙方提供的服务具体标准满足工业与信息化部颁布的《电信服务规范》及甲方要求，保证甲方使用乙方提供的业务安全畅通。

5.2乙方向甲方提供客户服务支撑电话4000111000，每天24小时受理甲方的故障申告，在甲方要求的时限内进行修复，甲方应积极予以协助配合。

5.3如乙方未按甲方要求时限内解决故障问题，甲方有权委托第三方处理，全部费用及甲方损失由乙方承担，甲方有权从合同款项中直接扣除，合同款项不足以扣除的，甲方有权向乙方追偿。

第六条　违约责任

6.1任何一方未履行本合同项下的任何一项条款均被视为违约。在此情形下,甲乙双方可就此问题进行协商,协商不成的,按本合同争议条款解决。

6.2甲乙双方任何一方任意终止合同给对方造成损失的，终止合同方应承担因此给对方造成的损失。

6.3乙方未按照合同（含附件）任一约定及甲方要求提供服务，均视为违约,每出现一次违约行为按本合同总额的千分之五向甲方支付违约金并赔偿甲方全部损失，同时，甲方有权委托第三方进行整改或处理，全部费用由乙方承担。乙方违约行为超过3次的，甲方有权解除本合同。

6.4因乙方原因导致合同终止或解除，乙方除退还甲方未服务期

限的费用外，仍需向甲方支付本合同总额5%的违约金并赔偿甲方全部损失（包含但不限于甲方经济损失、甲方支出律师费、保全保险费、差旅费及其他合理费用）。

6.5 甲方有可证明的合理原因，要求提前终止部分或全部服务，应提前四周向乙方提出书面申请。甲方按照终止日期向乙方付清服务费，多退少补。

第七条　知识产权

7.1 本合同履行过程中，甲方向乙方及乙方人员提供的信息、材料、技术等知识产权仍归甲方所有；本合同的签订与履行不代表甲方对乙方的知识产权转让和许可，乙方仅可出于为甲方提供服务之目的而使用。

7.2 因提供服务的需要，乙方提供给甲方任何材料的知识产权仍归乙方所有，甲方在接受服务的范围内有权使用；双方如另有约定的，以另外约定为准。

7.3 乙方保证为提供本合同服务所使用或涉及的相关设备、软件和技术资料等，均享有合法权利或已取得合法授权，如发生侵权等争议，乙方负责处理并承担由此引发的全部责任，如造成甲方损失，乙方负责双倍赔偿。

第八条 用户业务数据

8.1 乙方理解并认可，甲方通过乙方提供的服务，加工、存储、上传、下载、分发以及通过其他方式处理的数据（即在线数据），以及利用乙方可能配置的备份工具备份的数据（即离线数据）均为甲方的用户业务数据，甲方完全拥有甲方的用户业务数据。

8.2 就用户业务数据，乙方除执行甲方的服务要求外，不进行任何未获授权的使用及披露；

但以下情形除外：

8.3.1 在国家有关机关依法查询或调阅用户业务数据时，乙方具有按照相关法律法规或政策文件要求提供配合，并向第三方或者行政、司法等机构披露的义务，但乙方应提前书面告知乙方；

8.3.2 甲方和乙方另行协商一致。

8.4. 甲方可自行对甲方的在线数据进行删除、更改等操作。如甲方自行释放服务或删除在线数据的，乙方将立即实时删除甲方的在线数据，对应的离线数据（如有）按照甲方设定的备份规则（如未设定，则按乙方默认的规则）存储并删除。如甲方数据误删、更改等，乙方应全力协助甲方进行恢复。

第九条　权利义务的转让

除本协议另有约定外，任何一方未经对方事先书面同意，不得转让本合同项下的任何一项权利和义务。

第十条　保密义务

10.1 乙方在本协议生效前及本协议生效后通过任何方式接触或知悉的甲方的任何信息，以及虽属第三方但是甲方承担保密义务的信息具有保密义务。

10.2 以上保密信息的获得形式包括但不限于：甲方以数据、文字、图片及记载上述内容的资料、光盘、软件、图书等有型媒介体现，也可通过口头等视听形式传递。（2）乙方及乙方人员在双方合作过程中通过观察、测试、体验、分析等方式知悉。

10.3 上述保密义务在本合同终止或解除（无论何种原因）后仍应履行，直至保密信息被依法公开披露或称为公开信息之日止。

10.4 乙方如违反保密义务，视为违约，除向甲方支付违约金外，赔偿给甲方造成的一切损失。如乙方因违约而受有利益，则应将所得

利益支付给甲方。

第十一条　不可抗力

11.1 在合同有效期内，任何一方由于诸如战争、严重火灾、洪水、台风、地震等不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

11.2 不可抗力事件发生后，应立即通知对方，并在不可抗力事件结束后 3 日内以书面形式将不可抗力的情况和原因通知合同对方，并提供有关权威机构出具的证明文件。

11.3 不可抗力事件延续 30 天以上，双方应通过友好协商，确定是否继续履行合同。如双方协商终止合同，服务费用据实结算，于协议终止后 3 日内多退少补。

第十二条　通知

一方向另一方发出的书面信息，应按双方约定的通信地址以邮件或图文传真方式发送。任何一方对其联系方式的变更应及时书面通知对方。

第十三条　争议的解决

13.1 因履行本合同所产生的争议，任何一方可向甲方住所地人民法院提起诉讼。

13.2 除正在诉讼的争议事项外，双方应继续行使其本合同项下的其余权利，并履行其本合同项下的其它义务。

第十四条　合同期限及解除条款

14.1 本合同有效期壹年，服务周期为（2024 年 9 月 1 日-2025 年 8 月 31 日），自双方法定代表人或授权代表人签字并加盖公章或合同专用章之日起生效。

14.2 除本协议另有约定外，在合同有效期内，任何一方欲解除本合同，应提前 20 个工作日以书面形式向对方提出，经对方书面同意后方可解除本合同，但解除合同方应承担被解除方的损失。如合同到期、终止或解除，乙方应按甲方要求配合甲方对其系统、设备、数据进行搬迁、转移或销毁。乙方应妥善保留甲方数据，不得擅自销毁。

14.3 在本合同有效期内，若遇有国家法律、法规、政策调整或双方认为需要变更的条款，双方将根据国家法律、法规、政策变更合同内容或终止本合同。

第十五条 附则

15.1 本合同未尽事宜，按照国家有关规定执行。

15.2 未经甲乙双方书面确认，任何一方不得自行变更或修改本合同。

15.3 本合同一式陆份，甲方肆份，乙方贰份，具有同等法律效力。

15.4 本合同所有附件作为合同不可分割的组成部分，与合同正文具有同等法律效力。

甲方：（盖章）

法定代表人
或委托代理人签字：

联系方式：18637188605

签订日期：2024年11月23日

乙方：（盖章）

法定代表人
或委托代理人签字：

联系方式：18639552296

签订日期：2024年11月23日

附件一：服务内容及明细（含课程资源服务）

（1）资源需求

序号	类别	资源名称	资源需求	数量	单位
一、骨干云服务资源					
1	服务器资源相关	ECS服务器	CentOS 7.6及以上系统8核16G系统盘：50G SSD数据盘：200G 高性能磁盘（高效云盘）	3	项
2			CentOS 7.6及以上系统16核32G系统盘：50G SSD数据盘：100G 高性能磁盘（高效云盘）	12	项
3			CentOS 7.6及以上系统8核16G系统盘：50G SSD数据盘：100G 高性能磁盘（高效云盘）	6	项
4			CentOS 7.6及以上系统16核32G系统盘：50G SSD数据盘：200G 高性能磁盘（高效云盘）	4	项
5			CentOS 7.6及以上系统16核32G系统盘：50G SSD数据盘：2000G 高性能磁盘（高效云盘）	1	项
6			CentOS 7.6及以上系统8核32G系统盘：50G SSD数据盘：200G 高性能磁盘	1	项
7			CentOS 7.6及以上系统，4核32G系统盘：50G SSD数据盘：100G 高性能磁盘（高效云盘）	3	项
8			CentOS 7.6及以上系统16核32G系统盘：50G （SSD）数据盘：3T 高效云盘	1	项
9			CentOS 7.6及以上系统，8核16G系统盘：50G SSD数据盘：500G（高效云盘）	1	项
10			CentOS 7.6及以上系统，4核8G系统盘：50G SSD数据盘：200G（高效云盘）	1	项
11	数据	云数据库	主从	1	项

	库	RDS	16核32G 300G（SSD）		
12	网络	弹性公网IP	200M带宽	1	个
			5M带宽	2	个
			10M带宽	4	个
			20M带宽	1	个
			30M带宽	1	个
13	网络安全	主机安全		35	项
14		云漏洞扫描		1	项
15		堡垒机		35	项
16		云防篡改		3	项
17		云防火墙		1	项
18		WEB应用防火墙		1	项
19		日志审计		35	项
20		数据库审计		4	项
二、合营云服务资源					
1	对象存储OSS	存储包60TB+下行流量包1T		1	项
2	视频点播	转码后是1080P的视频，20w人在线学习，一个人学习2400分钟；视频存储5T		1	项
3	云服务器	8 vCPUs 16GB，系统盘ESSD：50G，数据盘高效云盘：500G，debian 12.6		1	项
4		8 vCPUs 16GB，系统盘ESSD：50G，数据盘高效云盘1：500G，数据盘高效云盘2：2T debian 12.6		1	项
5		16 vCPUs 32GB ，系统盘ESSD：50G，数据盘高效云盘：500G，debian 12.6		3	项
6		16 vCPUs 32GB ，系统盘ESSD：50G，数据盘高效云盘：200G，debian 12.6		3	项

7		16 vCPUs 32GB ，系统盘ESSD：50G，数据盘高效云盘：500G， Windows Server 2019 标准版 64位(标准版)	1	项
8		16 vCPUs 32GB 系统盘ESSD：50G，数据盘高效云盘：2TB，CentOS 7.6 64位	1	项
9	弹性公网IP	10M	4	条
10	容器K8S	pro版 版本1.30.1 网络插件terway node节点 ecs.g6.2xlarge (8 vCPU 32 GiB，通用型 g6) *8台 ESSD100G ESSD 100G	1	套
11		集群托管		
12		NAT网关		
13		API server SLB 高阶型I (slb.s3.small)		
14		EIP		
15	云数据库	mysql8.0 16 64 GB 600G存储，主从读写分离	1	项
16		redis 云原生盘 启用集群 8分片32G内存 redis7.0版本	1	项
17	消息队列kafka	标准版（高写版）alikafka.hw.3xlarge、高效云盘800G 、VPC实例	1	项
18	网络安全	云web应用防火墙	1	项
19		云防火墙	1	项
20		云堡垒机	1	项
21		云安全中心	1	项
22		云防篡改	1	项
23		云综合日志审计	1	项
24		云漏洞扫描	1	项

25		云数据库审计	1	项
26		SSL证书	1	个
三、安全评估服务				
1	安全评估服务	提供安全评估服务（详见技术参数要求）	1	项
四、短信服务				
1	短信服务	提供短信服务（详见技术参数要求）	1	项

（2）技术参数详细要求

序号	类别	名称	技术参数要求
一、骨干云服务资源			
1-10	服务器资源相关	ECS服务器	（1）支持对云服务器的创建、开机、关机、重启、VNC远程连接、修改VNC远程连接密码、修改私网IP、重置云服务器密码、变更规格、创建镜像、格式化操作系统、更换操作系统、更改安全组、绑定/解绑弹性公网IP、绑定/解绑IPv6带宽、绑定辅助网卡、克隆、手动续费、自动续费退订等功能。 （2）云服务使用管理平台需具备用户自助服务界面，用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作。通过自服务门户能够申请的服务包括但不限于云主机、云硬盘、云负载均衡、云数据库、对象存储等。 （3）云服务支持使用管理平台支持日志查看功能，查看云计算基础产品实例的名称、操作类型、操作结果、操作时间、资源拥有者，实现更细粒度管理。 （4）云服务使用管理平台能够集成安全资源池，满足租户级安全需求。 （5）云服务支持使用管理平台能够提供安全组服务，通过设置安全组实例的名称、描述、出入方向端口配置，用户可以对虚拟机之间的安全互访定义复杂且精细的流量路径，保证虚拟机互相访问的安全性。 （6）支持创建资源组，通过资源组功能可管控不同用户管理不同的云服务器资源。支持对创建的实例在

			控制台进行管理，可通过IP、ID进行查看、检索。 （7）支撑创建时可选镜像，支持私有镜像上传，支持常用镜像、公共镜像、私有镜像、共享镜像。 （8）支持在线虚拟机资源热添加，可以在线调整虚拟机的CPU、内存、硬盘等资源。 （9）提供安全组管理功能，创建安全组，灵活配置安全组规则，并支持查看安全组所关联的云服务器 ECS 实例信息、辅助网卡信息；支持导入/导出安全组规则。 （10）支持查看云服务器 ECS 的 CPU 使用率、内存使用率、云盘使用率、云盘读/写带宽、云盘读/写 IOPS、流入速率、流出速率监控信息。 （11）平台支持适配国产化操作系统，需提供截图证明，并加盖供应商公章。 关于高效云盘技术参数要求： （1）用户可以将单独创建的数据盘挂载到ECS实例上，可以将数据盘从ECS实例上卸载下来。 （2）当云盘容量不满足业务需要时，用户可进行弹性扩容。 （3）支持包年/包月云盘未到期退订、到期后删除，支持按量付费云盘删除。 （4）云盘、快照创建完成后可以修改名称。 （5）用户可以创建快照来快速保存指定时刻云盘的数据。 （6）用户可以通过快照创建新云盘，使新云盘在初始状态就具有快照中的数据。 （7）一旦升级或迁移过程中出现问题，用户可以通过快照及时将业务恢复到快照创建点的数据状态。 （8）用户可以删除不再需要的快照。 （9）支持通过单台云服务器挂载多块云硬盘的方式扩展存储空间，同时支持对单块云硬盘进行在线扩容。
11	数据库	云数据库RDS	（1）云数据库支持单机、主备、读写分离架构，支持5.7、8.0版本。 （2）支持每天一次的自动备份，在控制台上手动点击创建备份。 （3）支持 IP 白名单/安全组设置进行访问控制。

			（4）支持对服务续费，支持对服务退订，包括单机实例、主备实例、只读实例。 （5）支持在线重启数据库。 （6）支持创建、查看、删除账号、修改权限、重置密码，支持创建、查看、删除数据库、修改权限。 （7）支持开启、关闭数据库代理，从而使用读写分离功能，支持对代理节点的监控。 （8）支持设置安全组规则以支持内网访问。 （9）支持查看、修改参数信息、支持应用模板、导出模板、预览。 （10）支持查看、筛选操作日志。 （11）提供数据库服务实例的基础监控信息，包括资源监控和引擎监控。 （12）提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。 （13）云数据库数据存储持久性达99.99999999%以上（10个9），且能提供可信云官方网站证明截图。
12	网络	弹性公网IP	弹性公网 IP（Elastic IP Address）是可以独立购买和持有的静态 IP 地址资源，用户可以将弹性公网 IP 和弹性云服务器、裸金属服务器或是负载均衡进行绑定和解绑，实现专有网络 VPC 中的云服务器等实例通过公网 IP 地址与公网互通。
13	网络安全	主机安全	（1）防暴力破解：支持对暴力破解行为进行检测，并对触发云主机防暴力破解规则的行为进行拦截。 （2）入侵攻击防御：支持针对不同分组设备创建不同的入侵防御模板，在不同模板中添加相应的防御规则。 （3）主机防火墙：支持针对不同的安全要求设置防火墙的策略，保护主机免受网络攻击、端口扫描等。 （4）Webshell扫描模块：满足包含了不少于40万的网站后门样本和大量的后门特征码，双重机制保证对于样本的有效检测与查杀。 （5）安全基线：支持宿主机及云主机内扫描设定的检查项，对不合规项进行统计上报，同时系统给出相应的建议操作，保障云环境的安全合规。 （6）虚拟化加固：满足虚拟化加固功能通过海量样本特征和恶意行为分析引擎可以有效防护虚拟机逃

			逸、恶意破坏Hypervisor等行为，实现Hypervisor层的安全防护。 （7）网卡流量统计：支持网卡流量统计模块可以使管理员在控制中心清楚直观地查看各个主机网卡的流量情况，实现各主机流量的统一管理查看，快速定位存在流量异常的云服务器。 （8）权限管控：支持提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。 （9）病毒查杀引擎：支持依靠强大的云查杀引擎、启发引擎、脚本引擎等杀毒引擎，各引擎在运行时可进行数据交互，对主机进行扫描结果缓存共享，提升查杀精确度和效率。 （10）网络攻击防护：提供多参数、多协议的流量识别控制；可针对系统漏洞特征，实施“虚拟补丁”的入侵防御规则，抵御 0-day 漏洞攻击；同时增加暴力破解攻击的拦截，全面应对云环境中大量弱密码、数据库弱口令攻击。 （11）防病毒：支持快速扫描系统目录、系统启动项、浏览器配置、系统登录和服务、文件和系统内存。
14		云漏洞扫描	（1）数据库漏扫 提权漏洞、缓冲区溢出漏洞、访问控制漏洞、SQL 注入漏洞、执行权限过大漏洞、访问权限绕过漏洞等。 （2）系统漏扫 缓冲区溢出漏洞、拒绝服务攻击漏洞、危险服务、信息泄漏、弱口令等。 （3）实时告警 系统告警、邮件告警、短信告警。
15		堡垒机	（1）支持账号管理，支持可建立基于唯一身份标识的全局用户账户管理，支持统一账号管理策略，实现与各服务器、网络设备、安全设备、应用系统、数据库服务器等无缝连接。主要体现在身份管理、角色分权、会话协同和双人授权四个方面。 （2）支持访问控制，支持通过访问控制策略和命令控制策略，基于最小权限原则，实现集中有序的运维操作管控，让正确的人做正确的事。 （3）支持安全审计，支持基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控

			用户对目标资源的所有敏感操作，聚焦关键事件，实现对安全事件的实时发现与预警。 （4）支持多资产，支持传统的云主机的基础上还支持数据库和网络设备。 （5）支持多种网络协议，包括SSH、RDP、TELNET、VNC、FTP、SFTP、SCP、Rlogin 等。 （6）支持定期批量修改密码，支持可以根据账户、账户组、时间、改密周期、改密方式生成详细的改密计划，到期自动执行。 （7）支持自定义脚本并批量执行，防护方式更加灵活，不再受限于系统可定义的策略。 （8）支持指令级细粒度授权、运维全过程控制和视频回放，能够对运维人员和运维过程进行有效控制，避免运维安全风险，满足法律法规及等级保护合规审计需求。
16		云防篡改	（1）网页防篡改系统 支持对网页防篡改客户端和的自动探测功能。 采用基于文件过滤驱动保护技术、事件触发机制相结合方式。 （2）日志记录 系统支持网页防篡改日志功能，记录时间、设备、进程、文件名、攻击类型。
17		云防火墙	（1）支持通过源安全域、目的安全域、源MAC地址、目的MAC地址、源IP地址、目的IP地址、地理位置、用户、服务、应用、时间等维度对流量实现精细管控。 （2）支持深度安全检测，支持网络攻击防护、IPS入侵防御，具有灵活自定义漏洞/间谍软件特征功能，具备多维度的数据防泄密功能。 （3）支持建立完整的访问控制和安全隔离能力，解决对云资产的异常访问问题。 （4）实时入侵防御内置威胁检测引擎，可同步更新全网威胁情报，对来自互联网的威胁进行实时检测和阻断。 （5）业务关系可视可了解业务的分区、分组、资产、资产间的访问关系，以及用户流量的聚类分析。支持流量可视分析，最大程度保证策略的正确性。 （6）支持一体化安全策略，支持通过源安全域、目

			的安全域、源地址、目的地址、地理位置、用户、服务、应用、时间等维度对数据进行识别，并对相应的数据实现入侵防御、URL 过滤、文件过滤、内容过滤、邮件过滤等一体化安全策略配置。 （7）支持动态特征检测，支持多维动态特征异常检测引擎，将异常行为、恶意行为特征码通过多维度提炼，动态进行表达，使得特征表达更加全面、精准、有效，提高入侵防御系统的命中质量。
18		WEB应用防火墙	（1）支持WEB入侵防护，支持通过多种机制的分析检测，能够有效的阻断攻击，保证Web应用合法流量的正常传输。 （2）恶意扫描防护，支持主流扫描器恶意扫描防护，第一时间发现并阻断黑客扫描威胁，智能封锁黑客威胁IP，提升黑客攻击成本，降低黑客入侵用户内网的风险。 （3）DDOS防护满足，支持多种组合条件对CC攻击进行检测。当流量超出DDoS防护的默认清洗阈值后，自动触发流量清洗，实现攻击防护。 （4）IDP入侵检测防护，支持结合深度内容检测、安全防护、上网行为管理等技术的入侵检测防御系统。 （5）支持日志审计，支持内置独立的审计日志、流量日志、攻击日志及DDoS防护日志，实时掌握应用安全动态，对攻击件事的发生及追踪全面掌控。 （6）支持访问管理，提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。 （7）支持实时入侵防御，支持内置威胁检测引擎，可同步更新全网威胁情报，对恶意 IP 与域名条目进行监控，实现对来自互联网的威胁进行实时检测和阻断。
19		日志审计	（1）支持200多种设备和系统日志解析，包括了主流的网络设备、安全设备、OS、数据库、应用系统、虚拟化和云计算等，并可不断扩展。 （2）支持强大的即时查询，在亿级以上的日志中秒级完成搜索查询。系统既支持范化字段的搜索、也支持原始日志的搜索，还支持范化字段和原始内容的组合查询，支持迭代查询和回退，也可支持基于策略的查询。

			（3）支持基于安全监测、告警和响应技术的事件关联分析引擎。在关联规则的驱动下，SMARTTM事件关联分析引擎能够进行多种方式的事件关联，包括统计关联、逻辑关联、时序关联、单事件关联、多事件关联、递归关联等等。 （4）支持关联分析，系统对于发现的安全事件可以进行自动告警，告警内容支持用户自定义字段。告警方式包括邮件、Syslog、SNMP Trap等。系统为用户提供了告警列表和统计功能，用户可以按告警IP分布、告警等级、告警趋势等维度进行告警浏览，并可查看所有告警详细信息。 （5）支持提供管理各类设备资产的资产库。所有资产都以树形结构进行组织和展示，并能够以此作为权限分配的依据，实现针对资产信息的访问控制，满足资产监控的最小化权限原则。 （6）支持日志及事件采集、标准化（归一化）、过滤、归并的数据治理功能。采集管理是系统进行日志分析的基础，用户可以通过指定需要采集的目标、采集协议、采集方式进行日志采集，并对日志源进行管理，监测日志源采集情况、白名单等。 （7）支持通过界面实时查看来自网络中各种IT资源的日志情况。内置了大量的分析场景，用户无需学习，即可开展审计操作。也允许用户自定义场景，并对场景进行树型结构的分类和归档。 （8）支持灵活自定义的仪表板，同时内置丰富的仪表板主题，如：日志源事件分析仪表板，Windows事件分析仪表板，网络设备分析仪表板，防火墙事件概览分析仪表板，WEB事件概览分析仪表板，FTP服务器日志分析等，同时用户还可以根据需要进行自定义仪表板。
20		数据库审计	（1）支持对Oracle、MS-SQL、DB2、MYSQL、Cachｅ DB、 Sybase、POSTGRESQL、并支持达梦、人大金仓国产等主流数据库提供自动化评估、审计和保护功能，支持对多个系统的审计以及支持多个不同类型的云数据库审计。 （2）支持权限角色分离，如系统管理员负责设备的运行设置；审计员负责查看相关审计记录及规则违反情况；日志员负责查看整体设备的操作日志及规则的

			修改情况等。 （3）支持通过IP、用户、数据库客户端工具、时间、敏感对象、返回行数、系统对象、高危操作等多种元素细粒度监控的风险操作行为。系统通过数据库状态监控、SQL注入检测等方式，及时发现威胁数据库安全的潜在因素并及时阻断，从而保证数据库安全运行。对系统中的特定访问SQL语句进行黑白名单控制，在这些SQL语句出现时能够迅速告警。 （4）支持对所有存储的海量信息进行索引，根据任意关键字检索到所有相关信息，通过分区、分表、索引等机制实现海量数据收取、提取分析及快速处理能力。 （5）支持针对所有访问数据库主机的操作审计，在数据交互过程中进行实时分析并生成各类统计报表。提供等级保护合规报表以及自定义报表。 （6）支持提供对于所有行为能够进行事后查询、取证、调查分析，出具各种审计报表报告。 （7）支持提供对入侵和违规行为进行预警和告警，并能够指导管理员进行应急响应处理。
二、合营云服务资源			
1	对象存储OSS	对象存储OSS	（1）提供创建、查看、删除、列举存储空间等功能，方便用户管理存储空间。 （2）支持通过用户身份管理与访问控制服务（IAM）、Bucket权限管理、Object权限管理等方式进行权限访问控制。用户可根据需要灵活配置资源的读写权限。 （3）支持生命周期规则，用户可以将Bucket内过期的Object、碎片、历史版本删除，节省存储费用。 （4）支持灵活、多样、实时的图片处理服务，用户可将原始图片上传到对象存储中，通过在请求URL中增加处理参数，即可实时对图片进行处理，包括图片缩放、格式转换，添加水印等功能。 （5）支持使用兼容S3接口的SDK访问，用户只需设置访问密钥（AccessKeyId和SecretKey）以及访问域名（Endpoint），即可通过S3 SDK访问OSS。支持Java，Python，Javascript，等多种语言SDK。 （6）提供多种数据访问方式，用户可通过控制台、HTTP RESTful API、SDK 等多种途径，轻松便捷地访

			问。 （7）支持大规模在线升级，在线扩容，升级扩容过程中用户无感知，不影响用户业务。用户无需事先规划存储容量，存储空间可按需付费，弹性伸缩。 （8）支持版本管理，对于对象的覆盖和删除操作将会以历史版本的形式保存下来。这样用户在错误覆盖或者删除 Object 后，能够将 Object 恢复至历史版本。 （9）支持碎片管理，对象在分片上传过程中，如果未进行分片合并或终止操作，可能产生碎片，用户可以通过碎片管理功能，对碎片进行快速清理，节省存储空间。 （10）数据中心分布全国超过30个省和自治区，支持用户就近选择数据中心，利用对象存储的高带宽、低时延、高可用、低成本等特点，存储用户的海量数据。 （11）对象存储数据存储持久性99.9999999999%（12个9）以上，且能提供可信云官方网站证明截图。
2	视频点播	视频点播	①全球极速分发网络：以全球3200+个CDN节点、180 Tbps带宽输出能力，覆盖70多个国家和地区、支持数十家运营商。 ② 全方位加密保障：访问限制、播放鉴权、视频加密（阿里云加密、HLS加密、DRM加密）、安全下载等多重安全保障，防止盗链、非法下载等造成的损失，保障视频内容安全。
3-8	云服务器	云服务器	（1）支持对云服务器的创建、开机、关机、重启、VNC远程连接、修改VNC远程连接密码、修改私网IP、重置云服务器密码、变更规格、创建镜像、格式化操作系统、更换操作系统、更改安全组、绑定/解绑弹性公网IP、绑定/解绑IPv6带宽、绑定辅助网卡、克隆、手动续费、自动续费等功能。 （2）云服务器ECS提供的数据块级别的块存储产品，采用分布式三副本机制，为ECS实例提供99.9999999%的数据可靠性保证；其中系统盘配置NVMe ESSD云盘，具有较高的IOPS及较低的读写时延； （3）在同一可用区中，业务数据以多副本的形式分布存储在块存储集群中，保证读写过程中的数据稳定性，为ECS实例实现99.9999999%的数据可靠性保证；

			（4）可以通过定期创建快照，提高业务数据的安全性。快照是联通云备份产品，为云盘提供数据备份能力，确保日志和客户交易等信息有备份可查询。 （5）支撑创建时可选镜像，支持私有镜像上传，支持常用镜像、公共镜像、私有镜像、共享镜像。 （6）提供安全组管理功能，创建安全组，灵活配置安全组规则，并支持查看安全组所关联的云服务器 ECS 实例信息、辅助网卡信息； （10）支持查看云服务器 ECS 的 CPU 使用率、内存使用率、云盘使用率、云盘读/写带宽、云盘读/写 IOPS、流入速率、流出速率监控信息。 其中高效云盘的技术参数： （1）用户可以将单独创建的数据盘挂载到ECS实例上，可以将数据盘从ECS实例上卸载下来。 （2）当云盘容量不满足业务需要时，用户可进行弹性扩容。 （3）支持包年/包月云盘未到期退订、到期后删除，支持按量付费云盘删除。 （4）云盘、快照创建完成后可以修改名称。 （5）用户可以创建快照来快速保存指定时刻云盘的数据。 （6）用户可以通过快照创建新云盘，使新云盘在初始状态就具有快照中的数据。 （7）一旦升级或迁移过程中出现问题，用户可以通过快照及时将业务恢复到快照创建点的数据状态。 （8）用户可以删除不再需要的快照。 （9）支持通过单台云服务器挂载多块云硬盘的方式扩展存储空间，同时支持对单块云硬盘进行在线扩容。
9	弹性公网IP	弹性公网IP	弹性公网 IP（Elastic IP Address）是可以独立购买和持有的静态 IP 地址资源，用户可以将弹性公网 IP 和弹性云服务器、裸金属服务器或是负载均衡进行绑定和解绑，实现专有网络 VPC 中的云服务器等实例通过公网 IP 地址与公网互通。
10-14	容器k8s	容器k8s	（1）单集群支持千量级ECS节点。 （2）支持集群组件生命周期管理、支持集群手动和自动弹性伸缩。

			（3）支持存储卷的动态创建和迁移。 （4）提供高性能VPC/ENI网络插件，性能比普通网络方案提升20%。 （5）支持容器访问策略和流控限制。
15-16	云数据库	云数据库RDS	（1）云数据库支持单机、主备、读写分离架构，支持5.7、8.0版本。 （2）支持 IP 白名单/安全组设置进行访问控制。 （3）支持对服务续费，支持对服务退订，包括单机实例、主备实例、只读实例。 （4）高可用系列实例有一个备节点，根据所选参数模板的不同，主节点的数据会通过半同步或异步的方式同步到备节点，当主节点出现故障无法访问时，会自动切换到备节点。 （5）提供数据库服务实例的基础监控信息，包括资源监控和引擎监控。 （6）提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。 （7）高可用系列实例提供完整的产品功能，包括弹性伸缩、备份恢复、性能优化、读写分离等，保障核心数据的安全。
17	消息队列kafka	消息队列kafka	（1）兼容开源：云消息队列 Kafka 版100%兼容开源Apache Kafka，以直接使用开源Apache Kafka客户端与云消息队列 Kafka 版通讯。云消息队列 Kafka 版目前支持0.10.x~3.x的开源版本。 （2）无缝迁移：云消息队列 Kafka 版基于现有的开源Apache Kafka生态，无需任何代码改造，即可迁移上云。 （3）深度优化内核，解决开源版本千级分区性能瓶颈，支持万级分区性能不受损。 （4）支持秒级扩容。 （5）支持最高50 GB/s流量写入。 （6）支持灰度升级、升级/拖冷数据等极端场景写优化保障。 （7）全自动巡检运维体系保障，服务可用性达99.95%，数据可靠性达99.999999%。
18	网络安全	云web应用	（1）支持WEB入侵防护，支持通过多种机制的分析检测，能够有效的阻断攻击，保证Web应用合法流量的

		防火墙	正常传输。 （2）恶意扫描防护，支持主流扫描器恶意扫描防护，第一时间发现并阻断黑客扫描威胁，智能封锁黑客威胁IP，提升黑客攻击成本，降低黑客入侵用户内网的风险。 （3）DDOS防护满足，支持多种组合条件对CC攻击进行检测。当流量超出DDoS防护的默认清洗阈值后，自动触发流量清洗，实现攻击防护。 （4）IDP入侵检测防护，支持结合深度内容检测、安全防护、上网行为管理等技术的入侵检测防御系统。 （5）支持日志审计，支持内置独立的审计日志、流量日志、攻击日志及DDoS防护日志，实时掌握应用安全动态，对攻击件事的发生及追踪全面掌控。 （6）支持访问管理，提供IAM权限管控功能，不同子账号可给予全权限、只读权限、基本操作权限等不同权限，实现对资源操作的权限管控。 （7）支持实时入侵防御，支持内置威胁检测引擎，可同步更新全网威胁情报，对恶意 IP 与域名条目进行监控，实现对来自互联网的威胁进行实时检测和阻断。
19		云防火墙	①提供云防火墙的防御能力总览，展示最近7天访问流量统计数据和已检测出的安全风险统计数据。 ②支持公网资产的入方向和出方向流量的访问控制（南北向），有效防止外部恶意攻击和黑客入侵，并且严格控制主动外联的出流量。 ③支持对私网IP访问公网的流量进行访问控制，有效拦截内部网络到公网的未授权访问。
20		云堡垒机	①安全可靠的运维能力：堡垒机能在Windows、Linux系统上高效稳定地运维，在Windows系统上运维不卡顿、不漏审，并且实现了多云、线下IDC、跨VPC等混合云场景下服务器资产的统一管理、集中运维。 ②便捷实用、贴心服务：堡垒机简单、易用、高效。即买即开通，可根据需求进行灵活配置。支持一键启用，同时支持云服务器 ECS、云数据库RDS、PolarDB的一键同步，还有RAM用户、AD用户、LDAP用户的一键导入。
21		云安全中	（1）提供所有服务器的安全状态相关信息，例如服务器的防护状态、分组、地域、专有网络VPC等统计

		心	信息。 （2）支持一键检查，云安全中心会根据配置对指定服务器执行对应的检查，例如：漏洞检测、基线检测等。 （2）提供云产品安全状态的相关信息，包括存在风险云产品信息及云产品分类（负载均衡、云数据库RDS等）统计信息。 （3）提供所有网站的安全状态相关信息，主要包括网站根域名、子域名及其资产的风险状态和告警数量统计。 （4）WLinux软件漏洞检测对标CVE官方漏洞库，采用OVAL匹配引擎进行软件版本比对，对当前使用的软件版本中存在的漏洞进行告警。 （5）漏洞修复支持系统漏洞一键修复，同时自动化快照能力实现一键回滚，更安全地修复漏洞。 （6）Windows系统漏洞检测同步微软官网补丁源，对高危及有影响的漏洞进行检测和提醒。 （7）漏洞修复自动化识别漏洞修复所需的前置补丁包，解决服务器因无前置补丁而无法修复漏洞的问题，实现一键修复Windows漏洞。对需要重启系统修复的漏洞会进行提醒，提升修复Windows系统漏洞的效率。 （8）Web-CMS漏洞检测监控网站目录，识别通用建站软件，通过漏洞文件比对方式检测建站软件中的漏洞。 （9）提供针对网络上突然出现的紧急漏洞的检测服务。应急漏洞不支持一键修复，可以根据提供的修复建议，手动修复服务器上的应急漏洞。 （10）提供需紧急修复的漏洞聚合入口，帮助快速查看和修复所有高紧急程度的漏洞。 提供优先使用阿里云源进行漏洞修复的能力。打开该开关后，云安全中心会为自动选择阿里云的YUM/APT源配置，帮助提高漏洞修复成功率。
22		云防篡改	（1）网页防篡改系统 支持对网页防篡改客户端和的自动探测功能。 采用基于文件过滤驱动保护技术、事件触发机制相结合方式。 （2）日志记录

			系统支持网页防篡改日志功能，记录时间、设备、进程、文件名、攻击类型。
23		云综合日志审计	（1）支持200多种设备和系统日志解析，包括了主流的网络设备、安全设备、OS、数据库、应用系统、虚拟化和云计算等，并可不断扩展。 （2）支持强大的即时查询，在亿级以上的日志中秒级完成搜索查询。系统既支持范化字段的搜索、也支持原始日志的搜索，还支持范化字段和原始内容的组合查询，支持迭代查询和回退，也可支持基于策略的查询。 （3）支持基于安全监测、告警和响应技术的事件关联分析引擎。在关联规则的驱动下，SMARTTM事件关联分析引擎能够进行多种方式的事件关联，包括统计关联、逻辑关联、时序关联、单事件关联、多事件关联、递归关联等等。 （4）支持关联分析，系统对于发现的安全事件可以进行自动告警，告警内容支持用户自定义字段。告警方式包括邮件、Syslog、SNMP Trap等。系统为用户提供了告警列表和统计功能，用户可以按告警IP分布、告警等级、告警趋势等维度进行告警浏览，并可查看所有告警详细信息。 （6）支持日志及事件采集、标准化（归一化）、过滤、归并的数据治理功能。采集管理是系统进行日志分析的基础，用户可以通过指定需要采集的目标、采集协议、采集方式进行日志采集，并对日志源进行管理，监测日志源采集情况、白名单等。
24		云漏洞扫描	（1）数据库漏扫 提权漏洞、缓冲区溢出漏洞、访问控制漏洞、SQL 注入漏洞、执行权限过大漏洞、访问权限绕过漏洞等。 （2）系统漏扫 缓冲区溢出漏洞、拒绝服务攻击漏洞、危险服务、信息泄漏、弱口令等。
25		云数据库审计	（1）支持关联应用层和数据库层的访问操作，可以在C/S架构和B/S架构中使用应用身份识别功能。 （2）支持溯源应用者的身份和行为。 （3）支持分析高中低等级的风险、SQL注入、黑名单语句、违反授权策略等SQL行为。 （4）支持根据时间、客户端IP、客户端端口、服务

			端IP、服务端端口、数据库账号、资产信息、数据库实例、客户端工具、数据库类型、主机名等多角度分析会话。 （5）内置900+安全规则，覆盖常见的应用场景，并且在不断的丰富内置规则。支持自定义安全规则。 （6）内置安全规则包含已发现的不安全SQL语句的特征信息。数据库审计服务通过将审计到的SQL语句和安全规则进行匹配从而判断SQL语句中是否包含可疑行为。 （7）支持通过IP、用户、数据库客户端工具、时间、敏感对象、返回行数、系统对象、高危操作等多种元素细粒度定义要求监控的风险访问行为。
26		SSL证书	（1）支持证书申请、更新、吊销、续费等全生命周期管理。 （2）支持用户根据需求选择不同规格、品牌和类型的证书购买。 （3）支持证书上传、删除、续费、托管等能力。
三、安全评估服务			
1	信息安全	安全评估服务	1、风险评估：针对业务系统的弱点进行评估。应包含应用系统、操作系统、业务系统部署位置、安全域划分、安全设备防护等等评估内容。 在测试过程中将对可能发现的安全隐患给予说明，同时给出该隐患的解决建议。服务完毕后，出具《网络安全风险评估报告》。 2、人工验证：对所有安全隐患、威胁信息都要进行人工验证，保证不出现误报，验证完毕后，出具《系统整改建议书》，对所有检测过程发现的安全风险提出解决建议，并协助整改。
四、短信服务			
1	平台功能	短信发送	支持普通短信、超长短信（1900字）发送；
2			提供PC端自定义短信发送功能，支持EXCEL批量提交方式；
3			提供计划短信服务能力，支持按天、周、月、固定频率下发短信；
4			支持手机号码依照运营商过滤功能，用户可选择移动、电信、联通单网手机号码发送；
5			提供关键字、敏感词检测功能，可以实现下发前用户自查短信内容是否可发，提高短信下发效率；

6		双向短信	提供双向短信，支持双向短信发送、查询、导出等功能；
7		信息查询统计	支持任务短信查询，提供关闭任务短信审核从而取消任务短信发送功能；
8			提供按月查询短信发送明细记录，支持按照任务编号、手机号码、发送内容、状态、任务时间等维度条件查询、导出；
9			支持按照API维度、套餐分类维度、运营商维度、省份、签名维度从日、月、年层面统计及图形化呈现已发送及报告情况；
10		平台管理	支持接口发送、PC端页面发送等多种发送形式，短信发送平台具备短信群发、监控告警、携号转网、通道策略组及切换分流、黑白名单/关键词管理、短信查询统计等功能；
11	API接口	API接口	提供API账号管理能力，1个平台账号可以管理多个API账号；
12			提供SGIP、SMGP、CMPP2.0、3.0 、HTTP、WEBSERVICE、中间件（兼容国产系统）等短信提交方式；
13			提供短信群发（多号码同一内容短信群发或单号码单条短信发送）、申请签名、申请模板、报告拉取/推送、回复拉取/推送、余额查询等功能；
14			支持对短信号码及内容进行对称或非对称加密传输；
15			提供API白名单管理能力，配置后仅支持白名单内IP对应设备进行访问；
16	平台性能	平台性能	支持接口提交量支持每秒3000条；
17			平台日处理量级：千万级，在节假日等重大节日不影响发送速率及到达率；
18			平台响应时间：<10s
19			短信到达率：>99%（除去发送号码中状态不正常的用户，如空号、停机、关机、不在服务区等情况，统计每个自然月短信送达率，计算公式为：月短信按时送达率=短信平台发送成功的月短信总量/短信平台发出的月短信总量）
20			平台工作时间：7*24h*365