南阳市政务服务和大数据管理局政务云政府购买服务项目

投标文件

公共资源交易平台投标专用
AE2C1ACEC77646E1A62A8BC88EA14DB9

投　　标　　人：中国移动通信集团河南有限公司

法定代表人或委托代理人：

日　　期：　2023　年　12　月　22　日

目　录

一、开标一览表及资格证明文件 ····· 1
（一）开标一览表 ····· 1
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 1
（二）法定代表人（负责人）授权书（含法人代表（负责人）身份证、授权代表身份证） ····· 2
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 2
（三）关于资格的声明函 ····· 4
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 4
（四）投标人承诺函 ····· 5
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 5
（五）营业执照副本 ····· 7
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 7
（六）具有履行合同所必需的设备和专业技术能力的承诺 ····· 8
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 8
（七）依法缴纳税收和社会保障资金的缴费凭证（提供近半年内任意三个月的有效凭证） ····· 9
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 9
（八）良好的商业信誉和健全的财务会计制度的证明文件 ····· 12
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 12
（九）投标人出具2020年以来在经营活动中没有重大违法记录的书面声明（加盖单位公章） ····· 99
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 99
（十）投标人出具信用记录查询结果网页截图 ····· 100
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 100
（十一）投标人诚信承诺书 ····· 179
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 179
二、商务及技术文件 ····· 180
（一）投标书 ····· 180
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 180
（二）分项报价一览表 ····· 181
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 181
（三）项目技术方案、应急保障服务能力方案、承诺书等 ····· 191
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 191
（四）拟投入本项目的运维人员名单及基本情况 ····· 773
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 773
（五）技术偏差表 ····· 805
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 805
（六）商务偏差表 ····· 820
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 820
（七）投标人业绩 ····· 825
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 825
（八）投标人中小企业、监狱企业或残疾人福利性单位声明函（如果有的话） ····· 852
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 852
（九）招标文件要求的其它材料及投标人认为有必要提供的材料 ····· 854
1.南阳市政务服务和大数据管理局政务云政府购买服务项目 ····· 854

开标一览表

项目名称	南阳市政务服务和大数据管理局政务云政府购买服务项目
项目编号	南阳政采公开-2023-111
投标人	中国移动通信集团河南有限公司
投标报价	综合优惠率： 2.51 %
服务质量	合格，符合现行国家相关验收规范标准，达到采购人满意。
服务期限	3年
备注	无

注：“开标一览表”报综合优惠率

投 标 人（盖公章）：

2023 年12 月 22 日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA140B9

二、授权书

法定代表人（负责人）授权委托书

委托单位：中国移动通信集团河南有限公司

地址：郑州市经三路 48 号　　法定代表人（负责人）：楼向平

授权代表姓名：张航　性别：男　出生日期：1995 年 7 月 20 日

所在单位：中国移动通信集团河南有限公司南阳分公司

职务：解决方案经理

身 份 证：411303199507201017　现 住：河南省南阳市卧龙区卧龙岗乡刘洼村椿西组 272 号

兹委托 张航　参加 南阳市政务服务和大数据管理局政务云政府购买服务项目 项目事宜，并授权其全权办理以下事宜：

1、参加投标活动；

2、签订与中标事宜有关的合同。

授权代表在办理上述事宜过程中以其自己的名义所签署的所有文件我均予以承认。

授权代表无转委权。

委托期限：至上述事宜处理完毕止。

委托单位（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）（签字）：

授权代表（签字）：

时间：2023 年 12 月 22 日

公共资源交易平台投标专用

附：法定代表人（负责人）的身份证及授权代表的身份证

法定代表人身份证



此件仅供项目投标使用

授权代表身份证



此件仅供项目投标使用

三、资格声明函

关于资格的声明函

南阳市政府采购中心：

关于贵方编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目 公开招标，本签字人愿意参加投标，提供“采购内容及要求”中规定的服务，并证明提交的下列文件和说明是准确的真实的。

1、由 郑州市金水区 市场监管局签发的我方工商营业执照副本。

2、法定代表人（负责人）授权书。

3、法定代表人（负责人）或授权代表身份证（答疑时出示原件）。

4、公司地址、联系电话、传真等。

5、法定代表人（负责人）或授权代表的联系电话。

6、招标项目要求的其他文件。

7、本签字人确认资格文件中的说明是真实的、准确的。

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C196EC776A6E1162A8BC88EA14B89

四、承诺函

投标人承诺函

致：南阳市政府采购中心：

很荣幸能参与项目编号为：南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务 项目的投标。

我代表中国移动通信集团河南有限公司（投标人名称），在此作如下承诺：

1、完全理解和接受本项目招标文件的一切规定和要求；

2、我方递交的投标文件中所有的资料均为真实的、准确的，无任何虚假内容。若存在有虚假内容，我方愿意承担法律责任。

3、若中标，我方将按照招标文件的具体规定与采购人签订供货安装调试和售后服务合同，并且严格按合同履行义务，按时交付使用，保证设备质量符合招标文件要求，并提供优质服务。如果在合同执行过程中，发现问题，我方一定尽快对其进行调整，并承担相应的经济责任；

4、若中标，本承诺将成为合同不可分割的一部分，与合同具有同等的法律效力。

5、我方同意招标文件所附的合同文本作为与采购方签约的合同文本，非经双方一致同意，不得改变原合同文本的条款。

6、我方保证，严格遵守《中华人民共和国政府采购法》、《中华

公共资源交易平台投标专用
AE2C19CC77E46E1462A8C88FA14DB9

人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》及其他相关法律法规的规定，若有违反上述法律法规的行为，愿意接受处罚并承担相应的法律责任。

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9



统一社会信用代码

91410000719172532Q

营业执照

1-4

（副 本）

扫描二维码登录'国家企业信用信息公示系统'了解更多登记、备案、许可、监管信息。

名　　称　中国移动通信集团河南有限公司

类　　型　有限责任公司(外商投资企业法人独资)

法定代表人　楼向平

经营范围　经营基础电信业务和增值电信业务（上述经营项目的具体内容以工信部核发的有效许可证为准）。从事通信和互联网等网络的设计、投资和建设；通信和互联网等设施的安装、工程施工和维修；经营与通信和信息业务相关的系统集成、漫游结算清算、技术开发、技术服务、设备销售等；出售、出租通信终端设备、互联网设备及其零配件，并提供售后服务；房屋、柜台出租，商务代理服务；销售：家用电器、电子产品、智能设备、日用百货、五金、家具家居；设计、制作、发布、代理各类广告；电子商务平台运营；代收水电气暖费；票务代理。（依法须经批准的项目，经相关部门批准后方可开展经营活动）

注册资本　肆拾叁亿陆仟柒佰柒拾叁万圆整

成立日期　1999年08月06日

营业期限　1999年08月06日至2049年08月05日

住　　所　郑州市经三路48号

此件仅供投标使用

登记机关　郑州市金水区市场监督管理局

2022　07　28

年　月　日

http://www.gsxt.gov.cn

市场主体应当于每年1月1日至6月30日通过国家企业信用信息公示系统报送公示年度报告

国家企业信用信息公示系统网址：

国家市场监督管理总局监制

公共资源交易平台技术专用
AE1C19CEC77

六、具有履行合同所必需的设备和专业技术能力的承诺

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

我公司具有履行合同所必需的设备和专业技术能力。

本公司对上述承诺的真实性负责。如有虚假，依法承担相应法律责任。

特此承诺！

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C19CE...A6E1A62A8BC88...14DB9

七、依法缴纳税收和社会保障资金的缴费凭证 （提供近半年内任意三个月的有效凭证）

7.1 投标人 7-9 月依法缴纳税收的缴费凭证



中华人民共和国
税收完税证明

No.341005231000144264

填发日期：2023年 10月 20日　　国家税务总局郑州市金水区税务局第二税务分局

纳税人识别号	91410000719172532Q	纳税人名称	中国移动通信集团河南有限公司		
原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
34101623100035617	印花税	经济合同	2023-07-01至2023-09-30	2023-10-20	290.19
34101623100035617	印花税	经济合同	2023-07-01至2023-09-30	2023-10-20	42.96
34101623100035617	印花税	经济合同	2023-07-01至2023-09-30	2023-10-20	165,142.52
34101623100035617	印花税	经济合同	2023-07-01至2023-09-30	2023-10-20	18,811.17
34101623100035617	印花税	经济合同	2023-07-01至2023-09-30	2023-10-20	52,319.50
金额合计	（大写）人民币贰拾叁万陆仟陆佰零陆元叁角肆分				¥236,606.34

税务机关（盖章）征税专用章　　填票人 电子税务局　　备注：一般申报 正税自行申报，主管税务所（科、分局）：国家税务总局郑州市金水区税务局第二税务分局

妥善保管

收据联 交纳税人作完税证明



中华人民共和国
税收完税证明

No.341005231000144265

填发日期：2023年 10月 20日　　国家税务总局郑州市金水区税务局第二税务分局

纳税人识别号	91410000719172532Q	纳税人名称	中国移动通信集团河南有限公司		
原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
34101623100035617	印花税	经济合同	2023-07-01至2023-09-30	2023-10-20	66,978.89
34101623100035617	印花税	经济合同	2023-07-01至2023-09-30	2023-10-20	392,851.37
金额合计	（大写）人民币肆拾伍万玖仟捌佰叁拾元零贰角陆分				¥459,830.26

税务机关（盖章）征税专用章　　填票人 电子税务局　　备注：一般申报 正税自行申报，主管税务所（科、分局）：国家税务总局郑州市金水区税务局第二税务分局

妥善保管

收据联 交纳税人作完税证明

公共资源交易平台投标专用

7.2 投标人 8-10 月依法缴纳社会保障资金的缴费凭证



中华人民共和国
税收完税证明

No.441005230800001769

填发日期：2023年 8月 8日　　国家税务总局郑州市金水区税务局第二税务分局

纳税人识别号	91410000719172532Q	纳税人名称	中国移动通信集团河南有限公司

原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
441016230800254470	企业职工基本养老保险费	职工基本养老保险(个人缴纳)	2023-08-01至2023-08-31	2023-08-08	15,197,643.76
441016230800254470	失业保险费	失业保险(单位缴纳)	2023-08-01至2023-08-31	2023-08-08	149,615.08
441016230800254470	失业保险费	失业保险(个人缴纳)	2023-08-01至2023-08-31	2023-08-08	64,083.16
441016230800254470	基本医疗保险费	职工基本医疗保险(个人缴纳)	2023-08-01至2023-08-31	2023-08-08	427,945.08
441016230800254470	生育保险费	生育保险	2023-08-01至2023-08-31	2023-08-08	213,972.54
金额合计	(大写) 人民币壹仟陆佰零伍万叁仟贰佰伍拾玖元陆角贰分				¥16,053,259.62

税务机关（盖章）征税专用章　　填票人　电子税务局

备注：一般申报 正税自行申报，主管税务所（科、分局）：国家税务总局郑州市金水区税务局第二税务分局，社保编码：419900000356社保经办机构：河南省省本级医疗保障局

收据联 交纳税人作完税证明

妥善保管



中华人民共和国
税收完税证明

No.441005230900100829

填发日期：2023年 9月 5日　　国家税务总局郑州市金水区税务局第二税务分局

纳税人识别号	91410000719172532Q	纳税人名称	中国移动通信集团河南有限公司

原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
441016230900201115	企业职工基本养老保险费	职工基本养老保险(单位缴纳)	2023-09-01至2023-09-30	2023-09-05	30,580,738.56
441016230900201115	企业职工基本养老保险费	职工基本养老保险(个人缴纳)	2023-09-01至2023-09-30	2023-09-05	15,290,369.28
441016230900201115	失业保险费	失业保险(个人缴纳)	2023-09-01至2023-09-30	2023-09-05	64,083.16
441016230900201115	工伤保险费	工伤保险	2023-09-01至2023-09-30	2023-09-05	611,444.92
441016230900201115	生育保险费	生育保险	2023-09-01至2023-09-30	2023-09-05	215,808.54
金额合计	(大写) 人民币肆仟陆佰柒拾陆万贰仟肆佰肆拾陆元肆角陆分				¥46,762,444.46

税务机关（盖章）征税专用章　　填票人　电子税务局

备注：一般申报 正税自行申报，主管税务所（科、分局）：国家税务总局郑州市金水区税务局第二税务分局，社保编码：410000002050社保经办机构：河南省社会保障局

收据联 交纳税人作完税证明

妥善保管

公共资源交易平台投标专用
AE2C19DC7F0D4B248BC88EA14DB9

中华人民共和国
税收完税证明

No.441005231000150910

国家税务总局郑州市金水区税务局第二税务分局

填发日期：2023年 10月 9日 税务机关：

纳税人识别号	91410000719172532Q	纳税人名称	中国移动通信集团河南有限公司

原凭证号	税种	品目名称	税款所属时期	入(退)库日期	实缴(退)金额
4410162310001513960	企业职工基本养老保险费	职工基本养老保险(单位缴纳)	2023-10-01至2023-10-31	2023-10-09	30,516,974.72
4410162310001513960	失业保险费	失业保险(单位缴纳)	2023-10-01至2023-10-31	2023-10-09	151,025.60
4410162310001513960	失业保险费	失业保险(个人缴纳)	2023-10-01至2023-10-31	2023-10-09	64,687.60
4410162310001513960	基本医疗保险费	职工基本医疗保险(单位缴纳)	2023-10-01至2023-10-31	2023-10-09	1,727,471.60
4410162310001513960	基本医疗保险费	职工基本医疗保险(个人缴纳)	2023-10-01至2023-10-31	2023-10-09	431,867.90
金额合计	（大写）人民币叁仟贰佰捌拾玖万贰仟柒贰拾柒元肆角贰分				¥32,892,027.42

税务机关（盖章）征税专用章

填票人 电子税务局

备注：一般申报 正税自行申报，主管税务所（科、分局）：国家税务总局郑州市金水区税务局第二税务分局，社保编码：419900000356社保经办机构：河南省省本级医疗保障局

收据联 交纳税人作完税证明

妥善保管

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

八、良好的商业信誉和健全的财务会计制度的证明文件

8.1 2022 年度财务审计报告



中国移动通信集团河南有限公司

自 2022 年 1 月 1 日
至 2022 年 12 月 31 日止年度财务报表

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

KPMG Huazhen LLP
8th Floor, KPMG Tower
Oriental Plaza
1 East Chang An Avenue
Beijing 100738
China
Telephone +86 (10) 8508 5000
Fax +86 (10) 8518 5111
Internet kpmg.com/cn

毕马威华振会计师事务所
(特殊普通合伙)
中国北京
东长安街1号
东方广场毕马威大楼8层
邮政编码：100738
电话 +86 (10) 8508 5000
传真 +86 (10) 8518 5111
网址 kpmg.com/cn

审计报告

毕马威华振审字第 2303406 号

中国移动通信集团河南有限公司：

一、审计意见

我们审计了后附的第 1 页至第 72 页的中国移动通信集团河南有限公司 (以下简称“移动河南公司”) 财务报表，包括 2022 年 12 月 31 日的资产负债表、2022 年度利润表、现金流量表、所有者权益变动表以及相关财务报表附注。

我们认为，后附的财务报表在所有重大方面按照中华人民共和国财政部颁布的企业会计准则 (以下简称“企业会计准则”) 的规定编制，公允反映了移动河南公司 2022 年 12 月 31 日的财务状况以及 2022 年度经营成果和现金流量。

二、形成审计意见的基础

我们按照中国注册会计师审计准则 (以下简称“审计准则”) 的规定执行了审计工作。审计报告的“注册会计师对财务报表审计的责任”部分进一步阐述了我们在这些准则下的责任。按照中国注册会计师职业道德守则，我们独立于移动河南公司，并履行了职业道德方面的其他责任。我们相信，我们获取的审计证据是充分、适当的，为发表审计意见提供了基础。

三、管理层和治理层对财务报表的责任

管理层负责按照企业会计准则的规定编制财务报表，使其实现公允反映，并设计、执行和维护必要的内部控制，以使财务报表不存在由于舞弊或错误导致的重大错报。

KPMG Huazhen LLP, a People's Republic of China partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee.

毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所，是与英国私营担保有限公司 — 毕马威国际有限公司 ("毕马威国际") 相关联的独立成员所全球性组织中的成员。

公共资源交易平台投标专用
AE2C19CEC1C46...8BC88EA14DB9

KPMG

三、管理层和治理层对财务报表的责任 (续)

在编制财务报表时，管理层负责评估移动河南公司的持续经营能力，披露与持续经营相关的事项 (如适用)，并运用持续经营假设，除非移动河南公司计划进行清算、终止运营或别无其他现实的选择。

治理层负责监督移动河南公司的财务报告过程。

四、注册会计师对财务报表审计的责任

我们的目标是对财务报表整体是否不存在由于舞弊或错误导致的重大错报获取合理保证，并出具包含审计意见的审计报告。合理保证是高水平的保证，但并不能保证按照审计准则执行的审计在某一重大错报存在时总能发现。错报可能由于舞弊或错误导致，如果合理预期错报单独或汇总起来可能影响财务报表使用者依据财务报表作出的经济决策，则通常认为错报是重大的。

在按照审计准则执行审计工作的过程中，我们运用职业判断，并保持职业怀疑。同时，我们也执行以下工作：

(1) 识别和评估由于舞弊或错误导致的财务报表重大错报风险，设计和实施审计程序以应对这些风险，并获取充分、适当的审计证据，作为发表审计意见的基础。由于舞弊可能涉及串通、伪造、故意遗漏、虚假陈述或凌驾于内部控制之上，未能发现由于舞弊导致的重大错报的风险高于未能发现由于错误导致的重大错报的风险。

(2) 了解与审计相关的内部控制，以设计恰当的审计程序，但目的并非对内部控制的有效性发表意见。

(3) 评价管理层选用会计政策的恰当性和作出会计估计及相关披露的合理性。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A0CEA14DB9

KPMG

四、注册会计师对财务报表审计的责任 (续)

(4) 对管理层使用持续经营假设的恰当性得出结论。同时，根据获取的审计证据，就可能导致对移动河南公司持续经营能力产生重大疑虑的事项或情况是否存在重大不确定性得出结论。如果我们得出结论认为存在重大不确定性，审计准则要求我们在审计报告中提请报表使用者注意财务报表中的相关披露；如果披露不充分，我们应当发表非无保留意见。我们的结论基于截至审计报告日可获得的信息。然而，未来的事项或情况可能导致移动河南公司不能持续经营。

(5) 评价财务报表的总体列报 (包括披露)、结构和内容，并评价财务报表是否公允反映相关交易和事项。

我们与治理层就计划的审计范围、时间安排和重大审计发现等事项进行沟通，包括沟通我们在审计中识别出的值得关注的内部控制缺陷。

毕马威华振会计师事务所 (特殊普通合伙)　　中国注册会计师

谭亚红　谭亚红

中国 北京　　高林　高林

2023 年 3 月 23 日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A81C88EA14DB9

中国移动通信集团河南有限公司

资产负债表

2022 年 12 月 31 日

(金额单位：人民币元)

	附注	2022 年	2021 年
资产			
流动资产			
货币资金	6	2,583,296,896.55	4,636,127,685.66
应收票据		-	16,876,646.57
应收账款	7	3,104,860,155.14	2,161,334,196.13
预付款项		133,513,721.98	151,416,587.23
应收资金集中管理款	8	16,556,707,333.33	17,559,250,036.04
其他应收款	9	130,917,119.52	91,185,013.80
存货	10	178,687,975.51	286,517,857.08
合同资产	11	427,756,215.08	97,704,468.57
其他流动资产	12	147,164,898.14	836,348,171.05
流动资产合计		23,262,904,315.25	25,836,760,662.13

第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

公共资源交易平台专用
AE2C19CEC77646E1A62A8BC88EA14DB9

中国移动通信集团河南有限公司

资产负债表 (续)

2022 年 12 月 31 日

(金额单位：人民币元)

	附注	2022 年	2021 年
资产 (续)			
非流动资产			
长期股权投资	13	79,565,420.07	78,803,096.25
固定资产	14	36,372,933,005.84	35,207,976,319.33
在建工程	15	3,939,055,057.54	3,928,248,900.55
使用权资产	16	5,630,130,350.54	2,394,358,435.15
无形资产	17	1,829,821,413.88	1,810,044,283.76
开发支出		60,708,981.80	47,686,621.75
长期待摊费用	18	747,379,276.73	661,493,862.50
递延所得税资产	19	1,939,447,192.29	1,923,041,252.79
其他非流动资产	20	2,812,319,826.99	930,088,402.48
非流动资产合计		53,411,360,525.68	46,981,741,174.56
资产总计		76,674,264,840.93	72,818,501,836.69

公共资源交易平台专用
AE2C19CEC77646E1A62A8BC88EA14DB9

刊载于第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

中国移动通信集团河南有限公司

资产负债表 (续)

2022 年 12 月 31 日

(金额单位：人民币元)

	附注	2022 年	2021 年
负债和所有者权益			
流动负债			
应付票据	21	3,136,885,688.60	2,609,680,228.93
应付账款	22	14,595,248,270.39	14,711,674,546.57
预收款项	23	4,024,161,161.19	6,428,559,468.49
合同负债	24	2,669,729,741.42	2,731,594,502.15
应付职工薪酬	25	260,148,878.61	256,407,249.81
应交税费	5(5)	2,151,474,397.69	1,913,938,835.01
其他应付款	26	518,905,323.55	558,744,653.49
一年内到期的非流动负债	27	1,581,725,815.31	1,306,312,858.53
其他流动负债		42,786,646.24	47,658,548.35
流动负债合计		28,981,065,923.00	30,564,570,891.33
非流动负债			
租赁负债	28	4,047,335,810.01	1,116,843,341.76
长期应付款		1,996,425.11	1,812,384.63
长期应付职工薪酬		42,580,000.00	34,045,878.86
递延收益	29	310,555,268.08	278,843,969.34
其他非流动负债		1,523,589.96	2,049,551.58
非流动负债合计		4,403,991,093.16	1,433,595,126.17
负债合计		33,385,057,016.16	31,998,166,017.50

公共资源交易平台查验专用
AE2C19CEC77646E1A

刊载于第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

中国移动通信集团河南有限公司

资产负债表(续)

2022年12月31日

(金额单位:人民币元)

	附注	2022年	2021年
负债和所有者权益(续)			
所有者权益			
实收资本	30	4,367,733,640.58	4,367,733,640.58
资本公积	31	2,104,926,488.13	266,121,125.79
其他综合收益	32	(701,151.22)	(1,490,000.00)
盈余公积	33	16,045,661,439.33	16,045,661,439.33
未分配利润	34	20,771,587,407.95	20,142,309,613.49
所有者权益合计		43,289,207,824.77	40,820,335,819.19
负债和所有者权益总计		76,674,264,840.93	72,818,501,836.69

此财务报表已于2023年3月23日获董事会批准。

企业负责人	主管会计工作的公司负责人	会计机构负责人	(公司盖章)
(签名和盖章)	(签名和盖章)	(签名和盖章)	

刊载于第11页至第72页的财务报表附注为本财务报表的组成部分。

公共资源交易平台打印专用
AE2C19CEC77646E1A62A8BC88E14DB9

中国移动通信集团河南有限公司

利润表

2022 年度

(金额单位：人民币元)

	附注	2022 年	2021 年
营业收入	35	40,030,971,347.50	42,606,575,467.84
减：营业成本	35	(31,701,063,714.25)	(28,856,671,978.98)
税金及附加	36	(84,321,081.62)	(82,654,443.17)
销售费用		(2,629,701,047.59)	(2,797,401,037.82)
管理费用		(1,977,537,512.24)	(2,056,971,062.06)
研发费用		(166,428,842.68)	(111,807,967.83)
财务净收益	37	530,753,718.09	374,658,077.44
其中：利息收入		622,363,348.12	491,510,216.80
利息费用		(88,667,132.54)	(111,699,586.03)
加：其他收益	38	82,220,269.10	69,403,307.52
投资收益		762,323.82	(18,208,608.90)
信用减值损失	39	(176,154,972.60)	(336,166,251.68)
资产减值损失		(19,894,760.53)	(1,859,975.88)
营业利润		9,889,605,727.00	8,788,895,526.48
加：营业外收入	40(1)	147,478,488.21	94,208,670.39
减：营业外支出	40(2)	(23,631,055.05)	(276,939,635.80)
利润总额		10,013,453,160.16	8,606,164,561.07
减：所得税费用	41	(2,520,267,711.48)	(2,171,973,835.69)
净利润		7,493,185,448.68	6,434,190,725.38

刊载于第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

公共资源交易平台专用
AE2C19CEC77646E1A62A14DB9

中国移动通信集团河南有限公司

利润表（续）

2022 年度

（金额单位：人民币元）

	附注	2022 年	2021 年
（一）按经营持续性分类：			
持续经营净利润		7,493,185,448.68	6,434,190,725.38
（二）按所有权归属分类：			
归属于母公司所有者的净利润		7,493,185,448.68	6,434,190,725.38
其他综合收益的税后净额		788,848.78	(1,490,000.00)
（一）归属于母公司所有者的其他综合收益的税后净额		788,848.78	(1,490,000.00)
1.不能重分类进损益的其他综合收益		788,848.78	(1,490,000.00)
(1) 重新计量设定受益计划变动额		788,848.78	(1,490,000.00)
综合收益总额		7,493,974,297.46	6,432,700,725.38
归属于母公司所有者的综合收益总额		7,493,974,297.46	6,432,700,725.38

刊载于第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

中国移动通信集团河南有限公司

现金流量表

2022 年度

(金额单位：人民币元)

	附注	2022 年	2021 年
经营活动产生的现金流量：			
销售商品、提供劳务收到的现金		44,343,764,226.47	43,954,475,422.27
收到其他与经营活动有关的现金		274,703,158.84	229,756,412.71
经营活动现金流入小计		44,618,467,385.31	44,184,231,834.98
购买商品、接受劳务支付的现金		(23,941,824,224.21)	(20,250,815,520.36)
支付给职工以及为职工支付的现金		(3,968,565,525.58)	(3,813,200,129.65)
支付的各项税费		(2,399,707,536.53)	(2,405,464,775.84)
支付其他与经营活动有关的现金		(460,641,599.96)	(526,046,769.42)
经营活动现金流出小计		(30,770,738,886.28)	(26,995,527,195.27)
经营活动产生的现金流量净额	43(1)	13,847,728,499.03	17,188,704,639.71

公共资源交易平台技术专用
AE2C19CEC77646E1A62A8BC88EA14DB9

刊载于第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

中国移动通信集团河南有限公司

现金流量表(续)

2022年度

(金额单位:人民币元)

	附注	2022年	2021年
投资活动产生的现金流量:			
处置固定资产、无形资产和其他长期资产收回的现金净额		34,238,849.74	48,563,301.24
收到其他与投资活动有关的现金		6,773,766,254.85	11,775,649,998.54
投资活动现金流入小计		6,808,005,104.59	11,824,213,299.78
购建固定资产、无形资产和其他长期资产支付的现金		(9,914,716,577.07)	(9,399,801,775.17)
支付其他与投资活动有关的现金		(5,236,625,339.06)	(18,662,222,957.10)
投资活动现金流出小计		(15,151,341,916.13)	(28,062,024,732.27)
投资活动使用的现金流量净额		(8,343,336,811.54)	(16,237,811,432.49)

刊载于第11页至第72页的财务报表附注为本财务报表的组成部分。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

中国移动通信集团河南有限公司

现金流量表 (续)

2022 年度

(金额单位：人民币元)

	附注	2022 年	2021 年
筹资活动产生的现金流量：			
吸收投资收到的现金		1,823,536,074.45	-
筹资活动现金流入小计		1,823,536,074.45	-
分配利润或偿付利息支付的现金		(6,863,907,654.22)	(1,549,147,475.46)
支付其他与筹资活动有关的现金		(1,632,375,857.78)	(1,586,341,372.28)
筹资活动现金流出小计		(8,496,283,512.00)	(3,135,488,847.74)
筹资活动使用的现金流量净额		(6,672,747,437.55)	(3,135,488,847.74)
现金及现金等价物净增加额	43(3)	(1,168,355,750.06)	(2,184,595,640.52)
加：年初现金及现金等价物余额		3,260,263,507.18	5,444,859,147.70
年末现金及现金等价物余额	43(4)	2,091,907,757.12	3,260,263,507.18

刊载于第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

中国移动通信集团河南有限公司

所有者权益变动表

2022 年度

(金额单位：人民币元)

	附注	实收资本	资本公积	其他综合收益	盈余公积	未分配利润	所有者权益合计
2021 年 1 月 1 日余额		4,367,733,640.58	250,073,424.54	-	16,045,661,439.33	15,257,266,363.57	35,920,734,868.02
2021 年增减变动金额		-	16,047,701.25	(1,490,000.00)	-	4,885,043,249.92	4,899,600,951.17
1. 综合收益总额		-	-	(1,490,000.00)	-	6,434,190,725.38	6,432,700,725.38
2. 所有者投入资本	31	-	16,047,701.25	-	-	-	16,047,701.25
3. 利润分配		-	-	-	-	(1,549,147,475.46)	(1,549,147,475.46)
2021 年 12 月 31 日余额		4,367,733,640.58	266,121,125.79	(1,490,000.00)	16,045,661,439.33	20,142,309,613.49	40,820,335,719.19
2022 年增减变动金额		-	1,838,805,362.34	788,848.78	-	629,217,794.46	2,468,872,005.58
1. 综合收益总额		-	-	788,848.78	-	7,493,185,448.68	7,493,974,297.46
2. 所有者投入资本	31	-	1,838,805,362.34	-	-	-	1,838,805,362.34
3. 利润分配		-	-	-	-	(6,863,967,654.22)	(6,863,967,654.22)
2022 年 12 月 31 日余额		4,367,733,640.58	2,104,926,488.13	(701,151.22)	16,045,661,439.33	20,771,527,407.95	43,289,207,824.77

刊载于第 11 页至第 72 页的财务报表附注为本财务报表的组成部分。

公共资源交易平台投标专用
AE2619CEC7764B1462A8BC8EA14DB9

中国移动通信集团河南有限公司
财务报表附注
(金额单位：人民币元)

1 公司基本情况

中国移动通信集团河南有限公司（以下简称“本公司”），是经河南省工商行政管理局批准，由河南省移动通信局（以下简称“河南移动局”）与河南省移通实业有限公司（以下简称“实业公司”）共同出资，于 1999 年 8 月 6 日成立的有限责任公司，注册资本为人民币 10,000,000.00 元。注册地为河南郑州。

根据河南移动局及实业公司与中国移动通信集团有限公司（以下简称“中国移动集团公司”）签订的股权转让协议，河南移动局及实业公司于 1999 年将其在本公司所持有的全部股权转让予中国移动集团公司。

其后，中国移动集团公司将其拥有的在河南省的蜂窝移动电话网络业务，及经评估与业务相关的资产及负债于 1999 年 6 月 30 日通过中国移动（香港）集团有限公司及中国移动香港(BVI)有限公司，注入本公司，本公司的注册资本由人民币 10,000,000.00 元增加至人民币 4,367,733,640.58 元。

后根据本公司相关股东协议，于 2011 年 7 月 6 日，本公司的全部股权转由中国移动有限公司全资子公司中国移动通信有限公司持有，本公司于 2011 年 9 月 27 日获得变更后的中华人民共和国企业法人执照（统一社会信用代码为 91410000719172532Q）。

本公司主要从事经营基础电信业务和增值电信业务。从事通信和互联网等网络的设计、投资和建设；通信和互联网等设施的安装、工程施工和维修；经营与通信和信息业务相关的系统集成、漫游结算清算、技术开发、技术服务、广告业务、设备销售等；出售、出租通信终端设备、互联网设备及其零配件，并提供售后服务；房屋、柜台出租，商务代理服务。

本公司母公司为中国移动通信有限公司，最终控股公司为中国移动集团公司。

公共资源交易平台投标专用
AE2C19CEC77645H1...9BC88...A14DB9

2 财务报表编制基础

本公司以持续经营为基础编制财务报表。

(1) 遵循企业会计准则的声明

本财务报表符合财政部颁布的企业会计准则的要求，真实、完整地反映了本公司 2022 年 12 月 31 日的财务状况、2022 年度的经营成果及现金流量。

(2) 会计年度

本公司的会计年度自公历 1 月 1 日起至 12 月 31 日止。

(3) 记账本位币及列报货币

本公司记账本位币为人民币，本公司根据其经营所处的主要经济环境确定其记账本位币，本公司主要经营地区为中国内地，本财务报表以人民币列示。

3 主要会计政策和主要会计估计

(1) 外币折算

外币交易按交易发生日的中国人民银行（“央行”）基准汇率将外币金额折算为人民币入账。于资产负债表日，外币货币性项目采用资产负债表日的即期汇率折算为人民币。汇兑差额计入当期损益。以历史成本计量的外币非货币性项目，于资产负债表日采用交易发生日的即期汇率折算。以公允价值计量的外币非货币性项目，采用公允价值确定日的即期汇率折算。

(2) 现金和现金等价物

现金及现金等价物是指库存现金、可随时用于支付的存款，以及持有的期限短 (一般是指从购买日起 3 个月及以内到期) 、流动性强、易于转换为已知金额现金及价值变动风险很小的投资。

(3) 存货

(a) 分类

本公司的存货主要包括库存商品(包括设备、终端等)和周转材料等，按成本与可变现净值孰低计量。

公共资源交易平台投标专用
AE2C19C7C77646E1A6048BC88EA14DB9

(b) 发出存货的计价方法

存货于取得时按实际获取成本入账，发出存货的成本采用移动加权平均法计量。

(c) 存货可变现净值的确定依据及存货跌价准备的计提方法

存货跌价准备按存货成本高于其可变现净值的差额计提。可变现净值按日常活动中，以存货的估计售价减去估计的销售费用以及相关税费后的金额确定。

(d) 本公司的存货盘存制度采用永续盘存制。

(e) 周转材料的摊销方法

周转材料指能够多次使用但不确认为固定资产的低值易耗品、包装物和其他材料。周转材料通常于领用时采用一次转销法进行摊销，计入相关资产的成本或者当期损益。

(4) 长期股权投资及共同经营

长期股权投资包括本公司对联营企业的长期股权投资，联营企业为本公司能够对其财务和经营决策具有重大影响的被投资单位。本公司对联营企业投资采用权益法核算。

(a) 投资成本确定

以支付现金取得的长期股权投资，按照实际支付的购买价款作为初始投资成本。

(b) 后续计量及损益确认方法

采用权益法核算的长期股权投资，初始投资成本大于投资时应享有被投资单位可辨认净资产公允价值份额的，以初始投资成本作为长期股权投资成本；初始投资成本小于投资时应享有被投资单位可辨认净资产公允价值份额的，其差额计入当期损益，并相应调增长期股权投资成本。

采用权益法核算的长期股权投资，本公司按应享有或应分担的被投资单位的净损益和其他综合收益份额确认当期投资损益和其他综合收益。确认被投资单位发生的净亏损，以长期股权投资的账面价值以及其他实质上构成对被投资单位净投资的长期权益减记至零为限，但本公司负有承担额外损失义务且符合或有事项准则所规定的预计负债确认条件的，继续确认投资损失并作为预计负债核算。被投资单位除净损益、其他综合收益和利润分配以外股东权益的其他变动，调整长期股权投资的账面价值并计入资本公积。被投资单位分派的利润或现金股利于宣告分派时按照本公司应分得的部分，相应减少长期股权投资的账面价值。本公司与被投资单位之间未实现的内部交易损益按照持股比例计算

公共资源交易平台投标专用
AE2C19C[illegible]A62[illegible]C88EA14DB9

归属于本公司的部分予以抵销，在此基础上确认投资损益。本公司与被投资单位发生的内部交易损失，其中属于资产减值损失的部分，相应的未实现损失不予抵销。

(c) 确定对被投资单位具有共同控制及重大影响的依据

共同控制是指按照相关约定对被投资单位所共有的控制，并且被投资单位的相关活动必须经过分享控制权的参与方一致同意后才能决策。

重大影响是指对被投资单位的财务和经营政策有参与决策的权力，但并不能够控制或者与其他方一起共同控制这些政策的制定。

(d) 长期股权投资减值

对联营企业的长期股权投资，当其可收回金额低于其账面价值时，账面价值减记至可收回金额。

(e) 共同经营

共同经营是指本公司与其他合营方共同控制且本公司享有该安排相关资产且承担该安排相关负债的一项安排。

本公司主要按照下述原则确认与共同经营中利益份额相关的项目：

- 确认单独所持有的资产，以及按份额确认共同持有的资产；
- 确认单独所承担的负债，以及按份额确认共同承担的负债；
- 确认出售享有的共同经营产出份额所产生的收入；
- 按份额确认共同经营因出售产出所产生的收入；
- 确认单独所发生的费用，以及按份额确认共同经营发生的费用。

(5) 固定资产及在建工程

固定资产

(a) 固定资产的确认及初始计量

本公司的固定资产包括房屋及建筑物、通信设备 (如电信收发设备、交换中心及网络传输设备等) 、办公设备及其他等资产。

固定资产在与其有关的经济利益很可能流入本公司、且其成本能够可靠计量时予以确认。购置或新建的固定资产按取得时的成本进行初始计量。

公共资源交易平台专用
AE2C19CHC7646E1A62A8BC88EA14DB9

与固定资产有关的后续支出，在相关的经济利益很可能流入本公司且其成本能够可靠的计量时，计入固定资产成本，对于被替换的部分，终止确认其账面价值；所有其他后续支出于发生时计入当期损益。

(b) 固定资产的折旧方法

固定资产折旧采用年限平均法，按其入账价值减去预计净残值后在预计使用寿命内计提。对计提了减值准备的固定资产，则在未来期间按扣除减值准备及预计净残值后的账面价值及依据当可使用年限确定折旧额。

固定资产的预计使用寿命、预计净残值率及年折旧率列示如下：

	使用寿命	预计净残值率	折旧率
房屋及建筑物	8-30 年	3%	3.23%-12.13%
机器设备	5-10 年	0%-3%	9.70%-20.00%
运输工具	5-10 年	0%-3%	9.70%-20.00%
电子设备及其他资产	3-10 年	3%	9.70%-32.33%

对固定资产的预计使用寿命、预计净残值和折旧方法至少每年进行复核并作适当调整。

(c) 当固定资产的可收回金额低于其账面价值时，账面价值减记至可收回金额

(d) 固定资产的处置

当固定资产被处置，或者预期通过使用或处置不能产生经济利益时，终止确认该固定资产。固定资产出售、转让、报废或毁损的处置收入扣除其账面价值和相关税费后的金额计入当期损益。

在建工程

在建工程按实际发生的成本计量。实际成本包括建筑成本、安装成本、符合资本化条件的借款费用以及其他为使在建工程达到预定可使用状态所发生的必要支出。在建工程在达到预定可使用状态时，转入固定资产后开始计提折旧。当在建工程的可收回金额低于其账面价值时，账面价值减记至可收回金额。

(6) 租赁

租赁，是指在一定期间内，出租人将资产的使用权让与承租人以获取对价的合同。

公共资源交易平台股份专用
AE2C19CEC776462...62A8BC...EA14DB9

在合同开始日，本公司评估合同是否为租赁或者包含租赁。如果合同中一方让渡了在一定期间内控制一项或多项已识别资产使用的权利以换取对价，则该合同为租赁或者包含租赁。

(a) 本公司作为承租人

除土地使用权外，本公司的租赁业务主要包含通信铁塔租赁、房屋租赁、场地租赁及其他通信设备租赁。租赁合同通常为固定期限合同，一般无续约选择权。

在对包含租赁组成部分的合同开始或重新评估时，本公司根据各组成部分相对独立价格将合同对价分配至每个租赁和非租赁部分。除非本公司采用《企业会计准则第 21 号——租赁》允许的实务简化方法。

(i) 租赁负债的确认和计量

本公司的租赁负债按照租赁期开始日尚未支付的租赁付款额的现值确认。租赁付款额包括固定付款额，以及在合理确定将行使购买选择权或终止租赁选择权的情况下需支付的款项等。不与利率或指数挂钩的可变租金不纳入租赁付款额，在实际发生时计入当期损益。

在计算租赁付款额的现值时，折现率为租赁内含利率。无法确定租赁内含利率的，采用本公司增量借款利率作为折现率，在确定增量借款利率时，由于近期未获得第三方贷款融资，本公司在考虑租赁期及租赁信用风险的基础上，对无风险利率进行调整。租赁付款额在本金和融资费用之间进行分摊。本公司按照固定的周期性利率计算租赁负债利息，作为融资费用于租赁期内计入损益。本公司将自资产负债表日起一年内 (含一年) 支付的租赁负债，列示为一年内到期的非流动负债。

(ii) 使用权资产的确认和计量

使用权资产按照成本进行初始计量，该成本包括租赁负债的初始计量金额、租赁期开始日或之前已支付的租赁付款额、初始直接费用等，并扣除已收到的租赁激励。本公司能够合理确定租赁期届满时取得租赁资产所有权的，在租赁资产剩余使用寿命内计提折旧；若无法合理确定租赁期届满时是否能够取得租赁资产所有权，则在租赁期间与租赁资产剩余使用寿命两者孰短的期间内计提折旧。当可收回金额低于使用权资产的账面价值时，本公司将其账面价值减记至可收回金额。

公共资源交易平台专用
AE2C19CEC77[illegible]A8BC88[illegible]A14DB9

(iii) 租赁变更

租赁发生变更且同时符合下列条件时，本公司将其作为一项单独租赁进行会计处理：(1) 该租赁变更通过增加一项或多项租赁资产的使用权而扩大了租赁范围；(2) 增加的对价与租赁范围扩大部分的单独价格按该合同情况调整后的金额相当。

当租赁变更未作为一项单独租赁进行会计处理时，本公司在租赁变更生效日重新确定租赁期，并采用修订后的折现率对变更后的租赁付款额进行折现，重新计量租赁负债。租赁变更导致租赁范围缩小或租赁期缩短的，本公司相应调减使用权资产的账面价值，并将部分终止或完全终止租赁的相关利得或损失计入当期损益。其他租赁变更导致租赁负债重新计量的，本公司相应调整使用权资产的账面价值。

(iv) 其他租赁成本

对于租赁期不超过 12 个月的短期租赁和单项资产全新时价值较低的低价值资产租赁，本公司采用准则允许的简化处理，不确认使用权资产和租赁负债，将相关租金支出在租赁期内各个期间按照直线法计入当期损益或相关资产成本。

(v) 租赁现金流分类

本公司偿付短期租赁付款额、低价值资产租赁付款额和未计入租赁负债的可变租赁付款额计入经营活动现金流出。偿还租赁负债本金及利息所支付的现金计入筹资活动现金流出。

(b) 本公司作为出租人

实质上转移了与租赁资产所有权有关的几乎全部风险和报酬的租赁为融资租赁。其他的租赁为经营租赁。

经营租赁

本公司经营租出自有的房屋建筑物或设备等资产时，经营租赁的租金收入在租赁期内按照直线法确认。本公司将按销售额的一定比例确定的可变租金在实际发生时计入租金收入。当租赁发生变更时，本公司自变更生效日起将其作为一项新租赁，并将与变更前租赁有关的预收或应收租赁收款额作为新租赁的收款额。

(7) 无形资产

无形资产主要包括土地使用权、软件、电信服务频谱等，以成本计量。外购土地及建筑物的价款难以在土地使用权与建筑物之间合理分配的，全部作为固定资产。

公共资源交易平台投标专用
AE2619EC7A62A8DC88EA14DB9

对于使用寿命有限的无形资产，本公司将无形资产的成本扣除减值准备 (如有) 后按直线法在预计使用年限或受益期内摊销。除非该无形资产符合持有待售的条件。

无形资产的预计使用寿命列示如下：

	预计使用寿命
土地使用权	20-50 年
软件	2-5 年

对使用寿命有限的无形资产的预计使用寿命及摊销方法至少每年进行复核并作适当调整。

当无形资产的可收回金额低于其账面价值时，账面价值减记至可收回金额。

内部研究开发项目支出根据其性质以及研发活动最终形成无形资产按是否具有较大不确定性，被分为研究阶段支出和开发阶段支出。

研究阶段的支出，于发生时计入当期损益；开发阶段的支出，同时满足下列条件的，予以资本化：

(a) 完成该无形资产以使其能够使用或出售在技术上具有可行性；
(b) 具有完成该无形资产并使用或出售的意图；
(c) 无形资产如何产生经济利益的方式能够被证明；
(d) 有足够的技术、财务资源和其他资源支持，以完成该无形资产的开发，并有能力使用或出售该无形资产；以及
(e) 归属于该无形资产开发阶段的支出能够可靠地计量。

不满足上述条件的开发阶段的支出，于发生时计入当期损益。以前期间已计入损益的开发支出不在以后期间重新确认为资产。已资本化的开发阶段的支出在资产负债表上列示为开发支出，自该项目达到预定用途之日起转为无形资产。

(8) 长期待摊费用

长期待摊费用包括租入资产改良及其他已经发生但应由本期和以后各期负担的、分摊期限在一年以上的各项费用，按直线法在预计受益期内平均摊销，并以实际支出减去累计摊销后的净额列示。

公共资源交易平台投标专用
AE2C19CEC778...6FE1A62...BC88EA14DB9

(9) 金融工具

金融工具，是指形成一方的金融资产并形成其他方的金融负债或权益工具的合同。当本公司成为金融工具合同的一方时，确认相关的金融资产或金融负债。

(a) 金融资产

(i) 分类与计量

本公司根据管理金融资产的业务模式和金融资产的合同现金流量特征，将金融资产划分为：(1) 以摊余成本计量的金融资产；(2) 以公允价值计量且其变动计入其他综合收益的金融资产；(3) 以公允价值计量且其变动计入当期损益的金融资产。

金融资产在初始确认时以公允价值计量。对于以公允价值计量且其变动计入当期损益的金融资产，相关交易费用直接计入当期损益；对于其他类别的金融资产，相关交易费用计入初始确认金额。因销售产品或提供服务而产生的、未包含或不考虑重大融资成分的应收账款或应收票据，本公司按照预期有权收取的对价金额作为初始确认金额。

债务工具

本公司持有的债务工具是指从发行方角度分析符合金融负债定义的工具，分别采用以下三种方式进行计量：

- 以摊余成本计量

本公司管理此类金融资产的业务模式为以收取合同现金流量为目标，且此类金融资产的合同现金流量特征与基本借贷安排相一致，即在特定日期产生的现金流量，仅为对本金和以未偿付本金金额为基础的利息的支付。

本公司对于此类金融资产按照实际利率法确认利息收入，基于实际利率法计提的金融工具的利息包含在相应金融工具的账面余额中。此类金融资产主要包括货币资金、应收票据、应收账款和其他应收款等。

- 以公允价值计量且其变动计入其他综合收益

本公司管理此类金融资产的业务模式为既以收取合同现金流量为目标又以出售为目标，且此类金融资产的合同现金流量特征与基本借贷安排相一致。此类金融资产按照公允价值计量且其变动计入其他综合收益，但减值损失或利得、汇兑损益和按照实际利率法计算的利息收入计入当期损益。此类金融资产列示为其他债权投资，自

公共资源交易平台投标专用
AE2C19CE[illegible]

资产负债表日起一年内（含一年）到期的其他债权投资，列示为一年内到期的非流动资产；取得时期限在一年内（含一年）的其他债权投资列示为其他流动资产。

- 以公允价值计量且其变动计入当期损益

本公司将持有的未划分为以摊余成本计量和以公允价值计量且其变动计入其他综合收益的债务工具，以公允价值计量且其变动计入当期损益。在初始确认时，本公司为了消除或显著减少会计错配，将部分金融资产指定为以公允价值计量且其变动计入当期损益的金融资产。自资产负债表日起超过一年到期且预期持有超过一年的，列示为其他非流动金融资产，其余列示为交易性金融资产。

权益工具

本公司将对其没有控制、共同控制和重大影响的权益工具投资按照公允价值计量且其变动计入当期损益，列示为交易性金融资产；自资产负债表日起预期持有超过一年的，列示为其他非流动金融资产。此外，本公司将部分非交易性权益工具投资指定为以公允价值计量且其变动计入其他综合收益的金融资产，列示为其他权益工具投资。该类金融资产的相关股利收入计入当期损益。

(ii) 减值

本公司对于以摊余成本计量的金融资产、以公允价值计量且其变动计入其他综合收益的债务工具投资、合同资产等，以预期信用损失为基础确认损失准备。
本公司考虑有关过去事项、当前状况以及对未来经济状况的预测等合理且有依据的信息，以发生违约的风险为权重，计算合同应收的现金流量与预期能收到的现金流量之间差额的现值的概率加权金额，确认预期信用损失。

于每个资产负债表日，本公司对处于不同阶段的金融工具的预期信用损失分别进行计量。金融工具自初始确认后信用风险未显著增加的，处于第一阶段，本公司按照未来 12 个月内的预期信用损失计量损失准备；金融工具自初始确认后信用风险已显著增加但尚未发生信用减值的，处于第二阶段，本公司按照该工具整个存续期的预期信用损失计量损失准备；金融工具自初始确认后已发生信用减值的，处于第三阶段，本公司按照该工具整个存续期的预期信用损失计量损失准备。

如果金融工具的违约风险较低，欠款人在短期内履行其合同现金流量义务的能力很强，并且即便较长时期内经济形势和经营环境存在不利变化但未必一定降低欠款人履行其合同现金流量义务的能力，该金融工具被视为具有较低的信用风险。对于在

公共资源交易电子公共服务平台 AE2C19CE...

资产负债表日具有较低信用风险的金融工具，本公司假设其信用风险自初始确认后并未显著增加，按照未来 12 个月内的预期信用损失计量损失准备。

本公司对于处于第一阶段和第二阶段以及较低信用风险的金融工具，按照其未扣除减值准备的账面余额和实际利率计算利息收入。对于处于第三阶段的金融工具，按照其账面余额减已计提减值准备后的摊余成本和实际利率计算利息收入。

对于因销售商品、提供服务等日常经营活动形成的应收票据、应收账款和合同资产，无论是否存在重大融资成分，本公司均按照整个存续期的预期信用损失计量损失准备。对于应收租赁款，本公司亦选择按照整个存续期的预期信用损失计量损失准备。

当单项金融资产无法以合理成本评估预期信用损失的信息时，本公司依据信用风险特征将应收款项划分为若干类别组合，如应收个人客户组合、应收政企客户组合等，并在组合基础上计算预期信用损失。

对于划分为组合的应收账款、应收租赁款和因销售商品、提供劳务等日常经营活动形成的应收票据等，本公司参考历史信用损失经验，结合当前状况以及对未来经济状况的预测，通过违约风险敞口和整个存续期预期信用损失率，计算预期信用损失。除此以外的划分为组合的其他应收款，本公司参考历史信用损失经验，结合当前状况以及对未来经济状况的预测，通过违约风险敞口和未来 12 个月内或整个存续期预期信用损失率，计算预期信用损失。

本公司将计提或转回的损失准备计入当期损益。

(iii) 金融资产的终止确认

金融资产满足下列条件之一的，予以终止确认：(1) 收取该金融资产现金流量的合同权利终止；(2) 该金融资产已转移，且本公司将金融资产所有权上几乎所有的风险和报酬转移给转入方；(3) 该金融资产已转移，虽然本公司既没有转移也没有保留金融资产所有权上几乎所有的风险和报酬，但是放弃了对该金融资产的控制。

其他权益工具投资终止确认时，其账面价值与收到的对价以及原直接计入其他综合收益的公允价值变动累计额之和的差额，计入留存收益；除其他权益工具之外的金融资产终止确认时，其账面价值与收到的对价以及原直接计入其他综合收益的公允价值变动累计额之和的差额，计入当期损益。

公共资源交易平台专用
AE2C19CE0[illegible]18BC88EA14DB9

如果本公司不再合理预期金融资产合同现金流量能够全部或部分收回，则直接减记该金融资产的账面余额。这种减记视为相关金融资产的终止确认。这种情况通常发生在本公司确定债务人没有资产或收入来源可产生足够的现金流量以偿还将被减记的金额。但是，本公司的到期款项收回的程序仍会影响被减记的金融资产，如已减记的金融资产以后又收回的，则作为减值损失的转回计入收回当期的损益。

(b) 金融负债

金融负债于初始确认时分类为以摊余成本计量的金融负债和以公允价值计量且其变动计入当期损益的金融负债。

本公司的金融负债主要为以摊余成本计量的金融负债，包括应付票据、应付账款、其他应付款、租赁负债等。该类金融负债按其公允价值扣除交易费用后的金额进行初始计量，并采用实际利率法进行后续计量。期限在一年以下 (含一年) 的，列示为流动负债；期限在一年以上但自资产负债表日起一年内 (含一年) 到期的，列示为一年内到期的非流动负债；其余列示为非流动负债。

当金融负债的现时义务全部或部分已经解除时，本公司终止确认该金融负债或义务已解除的部分。终止确认部分的账面价值与支付对价之间的差额，计入当期损益。

(c) 金融工具的公允价值确定

存在活跃市场的金融工具，以活跃市场中的报价确定其公允价值。不存在活跃市场的金融工具，采用估值技术确定其公允价值。在估值时，本公司采用在当前情况下适用并且有足够可利用数据和其他信息支持的估值技术，选择与市场参与者在相关资产或负债的交易中所考虑的资产或负债特征相一致的输入值，并尽可能优先使用相关可观察输入值。在相关可观察输入值无法取得或取得不切实可行的情况下，使用不可观察输入值。

(d) 金融资产和金融负债的抵销

金融资产和金融负债应当在资产负债表内分别列示，不得相互抵销。但同时满足下列条件的，应当以相互抵销后的净额在资产负债表内列示：(1) 公司具有抵销已确认金额的法定权利，且该种法定权利是当前可执行的；(2) 公司计划以净额结算，或同时变现该金融资产和清偿该金融负债。不满足终止确认条件的金融资产转移，转出方不得将已转移的金融资产和相关负债进行抵销。

(e) 权益工具

权益工具，是指能证明拥有某个企业在扣除所有负债后的资产中的剩余权益的合同。在同时满足下列条件的情况下，本公司将发行的金融工具分类为权益工具：(1) 该金融工具

公共资源交易平台技标专用
AE2C19C6571...462AC...A14DB9

应当不包括交付现金或其他金融资产给其他方，或在潜在不利条件下与其他方交换金融资产或金融负债的合同义务；(2) 将来须用或可用公司自身权益工具结算该金融工具。

(10) 长期资产减值准备

固定资产、在建工程、使用权资产、无形资产及对联营企业的长期股权投资等，于资产负债表日存在减值迹象的，进行减值测试。对未达到可使用状态的无形资产，无论是否存在减值迹象，至少每年进行减值测试。减值测试结果表明资产的可收回金额低于其账面价值的，按其差额计提减值准备并计入资产减值损失。可收回金额为资产的公允价值减去处置费用后的净额与资产预计未来现金流量的现值两者之间的较高者。长期资产减值准备按单项资产为基础计算并确认，如果难以对单项资产的可收回金额进行估计的，以该资产所属的资产组确定资产组的可收回金额。资产组是能够独立产生现金流入的最小资产组合。

上述资产减值损失一经确认，以后期间不予转回。

(11) 公允价值的计量

除特别声明外，本公司按下述原则计量公允价值：

公允价值是指市场参与者在计量日发生的有序交易中，出售一项资产所能收到或者转移一项负债所需支付的价格。

本公司估计公允价值时，考虑市场参与者在计量日对相关资产或负债进行定价时考虑的特征(包括资产状况及所在位置、对资产出售或者使用的限制等)，并采用在当前情况下适用并且有足够可利用数据和其他信息支持的估值技术。使用的估值技术主要包括市场法、收益法和成本法。

(12) 职工薪酬

职工薪酬是本公司为获得职工提供的服务或解除劳动关系而给予的各种形式的报酬或补偿，包括短期薪酬、离职后福利、辞退福利和其他长期职工福利等。

(a) 短期薪酬

短期薪酬包括工资、奖金、津贴和补贴、职工福利费、医疗保险费、工伤保险费、生育保险费、住房公积金、工会和职工教育经费等。按照中国内地有关法规，本公司职工参加了由政府机构设立管理的社会保障体系，本公司为职工缴纳基本医疗保险、工伤保险和生育保险等社会保险费用及住房公积金。

公共资源交易平台投标专用
AE2C19C[illegible]C46E1[illegible]62A8BC[illegible]A14DB9

本公司在职工提供服务的会计期间，将实际发生或按规定的基准和比例计提的短期薪酬确认为负债，并计入当期损益或相关资产成本。其中，非货币性福利按照公允价值计量。

(b) 离职后福利

本公司将离职后福利计划分为设定提存计划和设定受益计划。设定提存计划是本公司向独立的基金缴存固定费用后，不再承担进一步支付义务的离职后福利计划；设定受益计划是除设定提存计划以外的离职后福利计划。于报告期内，本公司的离职后福利主要是为职工缴纳的基本养老保险、失业保险、企业年金及补充退休福利等，除补充退休福利外均属于设定提存计划。

养老保险

本公司中国内地职工参加了由当地劳动和社会保障部门组织实施的社会基本养老保险。本公司以当地规定的社会基本养老保险缴纳基数和比例，按月向当地社会基本养老保险经办机构缴纳养老保险费。职工退休后，当地劳动及社会保障部门有责任向已退休员工支付社会基本养老金。本公司在职工提供服务的会计期间，将根据上述社保规定计算应缴纳的金额确认为负债，并计入当期损益或相关资产成本。

年金

年金为本公司符合条件的员工加入的一项由中国移动公司公司统一安排的由第三方保险机构管理的退休计划，按员工薪资的一定比例或按年金相关之条款由本公司作出供款，供款在其发生时计入当期损益。

补充退休福利

除参加由当地劳动和社会保障部门组织实施的设定提存计划外，本公司根据相关政策规定向满足一定条件的已退休职工提供一项补充退休福利计划。在该计划下，本公司按照一定标准每年向退休职工发放或报销一定的补贴及医疗费用等。本公司将该计划下的未来支付义务折现后确认为负债，并计入损益。因精算假设变化等重新计量该项负债而产生的变动计入其他综合收益。

公共资源交易平台技术专用
AE2C19CEC77648[illegible]A8BC88[illegible]A14DB9

(c) 辞退福利

本公司在职工劳动合同到期之前解除与职工的劳动关系，或者为鼓励职工自愿接受裁减而提出给予补偿，在本公司不能单方面撤回解除劳动关系计划或裁减建议时和确认与涉及支付辞退福利的重组相关的成本费用时两者孰早日，确认因解除与职工的劳动关系给予补偿而产生的负债，同时计入当期损益。

(13) 股份支付

本公司实施的股票期权计划作为以权益结算的股份支付进行核算。

以权益结算的股份支付换取职工提供的服务的，以授予职工权益工具的公允价值计量。本公司授予的股票期权需完成等待期内的服务或达到规定业绩条件才可行权。在等待期内每个资产负债表日，本公司根据最新取得的可行权职工人数变动、预计是否达到规定业绩条件等后续信息对可行权权益工具数量作出最佳估计，并以此为基础，按照授予日的公允价值，将当期取得的服务计入当期损益，相应增加资本公积。后续信息表明可行权权益工具的数量与以前估计不同的，将进行调整，并在可行权日调整至实际可行权的权益工具数量。对于最终未能达到可行权条件的股份支付，本公司不确认成本或费用。在行权日，根据实际行权的权益工具数量，计算确定应转入股本的金额，将其转入股本。

本公司采用二项式期权定价模型确定股票期权的公允价值，基于授予日普通股股价等信息和参数确定股票期权的单位公允价值。

(14) 递延所得税资产和递延所得税负债

递延所得税资产和递延所得税负债根据资产和负债的计税基础与其账面价值的差额 (暂时性差异) 计算确认。对于按照税法规定能够于以后年度抵减应纳税所得额的可抵扣亏损，确认相应的递延所得税资产。对于商誉的初始确认产生的暂时性差异，不确认相应的递延所得税负债。对于既不影响会计利润也不影响应纳税所得额 (或可抵扣亏损) 的非企业合并的交易中产生的资产或负债的初始确认形成的暂时性差异，不确认相应的递延所得税资产和递延所得税负债。于资产负债表日，递延所得税资产和递延所得税负债按照预期收回该资产或清偿该负债期间的适用税率计量。

递延所得税资产的确认以很可能取得用来抵扣可抵扣暂时性差异、可抵扣亏损和税款抵减的应纳税所得额为限。

公共资源交易平台投标专用
AE2C19CE0176462...9C88EA14DB9

对与联营企业投资相关的应纳税暂时性差异，确认递延所得税负债，除非本公司能够控制该暂时性差异转回的时间且该暂时性差异在可预见的未来很可能不会转回。对与联营企业投资相关的可抵扣暂时性差异，当该暂时性差异在可预见的未来很可能转回且未来很可能获得用来抵扣可抵扣暂时性差异的应纳税所得额时，确认递延所得税资产。

资产负债表日，有确凿证据表明未来很可能满足获得足够的应纳税所得额用来抵扣可抵扣暂时性差异的，应当确认以前期间未确认的递延所得税资产。除因直接计入股东权益(包括其他综合收益)的交易或者事项产生的所得税影响计入股东权益外，本公司将当期所得税和递延所得税计入当期损益。

同时满足下列条件的递延所得税资产和递延所得税负债以抵销后的净额列示：

(a) 递延所得税资产和递延所得税负债与同一税收征管部门对本公司内同一纳税主体征收的所得税相关；

(b) 本公司内该纳税主体拥有以净额结算当期所得税资产及当期所得税负债的法定权利。

(15) 预计负债

因产品质量保证、亏损合同等形成的现时义务，当履行该义务很可能导致经济利益的流出，且其金额能够可靠计量时，确认为预计负债。

预计负债按照履行相关现时义务所需支出的最佳估计数进行初始计量，并综合考虑与或有事项有关的风险、不确定性和货币时间价值等因素。对于货币时间价值影响重大的，预计负债以预计未来现金流量折现后的金额确定最佳估计数；因随着时间推移所进行的折现还原而导致的预计负债账面价值的增加金额，确认为利息费用。
于资产负债表日，对预计负债的账面价值进行复核并作适当调整，以反映当前的最佳估计数。

预期在资产负债表日起一年内需支付的预计负债，列示为其他流动负债。

(16) 收入确认

本公司主要通过与客户签订可取消的月度合同或通常需缴纳预付款且/或存在提前离网罚金的固定服务期合同，向客户提供语音、数据和其他通信服务，并向客户销售通信相关的产品。

对于本公司提供的通信服务、通信相关产品及/或其他服务/产品，若客户可以从这些服务或产品中获益，且本公司转让这些服务或产品的承诺是可以单独识别的，则本公司将其识别为单项履约义务。

公共资源交易平台投标专用
AE2C19C2E276E1A6218BC8E2A14DB9

收入根据本公司转移所承诺的履约义务给客户时，有权获取且在合同中明确规定的交易对价来衡量，不包括代表第三方收取的金额。交易对价一般在合同中明确规定且不包含重大融资成分。

当对一项服务或商品的控制权转移给客户时，收入具体确认方式如下：

(a) 每项履约义务的收入于本公司向客户承诺的服务或商品转移给客户时，即完成履约义务时确认。一般情况下，当电信服务提供至客户过程中，客户获得对服务的控制权，本公司确认收入；于产品转移至客户时点，客户获得产品的控制权，本公司确认收入。

(b) 对于提供包括服务及产品等多项履约义务合同，本公司基于相对单独售价将交易对价分配至每项履约义务。服务及产品的相对单独售价主要基于可观察的销售价格。若单独售价不可直接观察时，本公司基于可合理获取的所有信息并最大限度地使用可观察数据估计单独售价。每项履约义务的收入于承诺的服务或产品的控制权转移给客户时确认。

(c) 本公司通常在服务及产品转移给客户前控制该服务和产品。在某些情况下，本公司在考虑合同的主要责任、销售定价和存货风险后，决定本公司是否作为主要责任人或代理人。如果在服务或产品转让给客户前，本公司评估认为未获取控制权，则本公司作为履行履约义务的代理人，收入按照预期有权收取的佣金或手续费净额确认。

合同资产主要与本公司向客户提供服务或产品而有权向客户收取对价的权利相关，且于报告日本公司未获得无条件收款权。当服务已提供且账单开具时，合同资产被重分类为应收账款。当在向客户提供合同中承诺的服务及产品前，本公司若已收到对价，则产生合同负债。合同负债主要包含向客户收取的通常不会返还的预付服务费用、客户积分奖励计划（“积分计划”）中未兑换的积分奖励以及未使用的递延流量。本公司收到的可返还的预付服务费用确认为预收款项。

(17) 合同成本

合同成本包括合同取得成本和合同履约成本。合同取得成本是指本公司为取得合同而发生的增量成本，主要包括应付第三方代理商的销售佣金，如果预期可收回，按照与客户合同取得成本相关的服务或产品向客户转移方式相同的基础在预期合同存续期内摊销，并计入销售费用。在实际应用中，如果摊销期限不超过一年，则在发生时确认为费用。为取得合同产生的资本化增量成本计入其他非流动资产。

公共资源交易平台 技术专用
AE2C19CEC7[illegible]162A8BC[illegible]A14DB9

合同履约成本是指本公司已发生的与履行通信服务合约直接相关、但不属于其他会计准则范围的成本。如果预期可收回，按照与客户合同履约成本相关的服务或产品向客户转移方式相同的基础在预期合同存续期内摊销，并计入营业成本。基于摊销期限，合同履约成本计入存货或其他非流动资产。

(18) 政府补助

政府补助是本公司从政府无偿取得的货币性资产或非货币性资产，包括税费返还、财政补贴等。国家相关文件规定作为资本公积处理的政府的专项拨款，不作为政府补助处理。

政府补助在本公司能够满足其所附的条件并且能够收到时，予以确认。政府补助为货币性资产的，按照收到或应收的金额计量。政府补助为非货币性资产的，按照公允价值计量；公允价值不能可靠取得的，按照名义金额计量。

与资产相关的政府补助，是指本公司取得的、用于构建或以其他方式形成长期资产的政府补助。与收益相关的政府补助是指除与资产相关的政府补助之外的政府补助。

与资产相关的政府补助，本公司将其确认为递延收益，并在相关资产使用寿命内按照合理、系统的方法分摊计入损益；与收益相关的政府补助，用于补偿以后期间的相关成本费用或损失的，确认为递延收益，并在确认相关成本费用或损失的期间，计入当期损益；若用于补偿已发生的相关成本费用或损失的，直接计入当期损益。

本公司对同类政府补助采用相同的列报方式。与日常活动相关的政府补助计入其他收益，与日常活动无关的政府补助计入营业外收支。

(19) 利润分配

资产负债表日后，经审议批准的利润分配方案中拟分配的利润，不确认为资产负债表日的负债，在附注中单独披露。

(20) 关联方

一方控制、共同控制另一方或对另一方施加重大影响，以及两方或两方以上同受一方控制、共同控制的，构成关联方。关联方可为个人或企业。仅仅同受国家控制而不存在其他关联方关系的企业，不构成关联方。

此外，本公司同时根据证监会颁布的《上市公司信息披露管理办法》确定本公司或本公司的关联方。

公共资源交易平台交易专用
AE2C19CE67[illegible]CF1A62A8BC88EA14DB9

(21) 分部信息

经营分部是本公司能够在日常活动中产生收入、发生费用的组成部分。本公司的经营分部是以主要经营决策者定期审阅的以进行资源分配及业绩评估为目的的内部财务报告为基础而确定。本公司的执行董事已被认定为主要经营决策者。

在报告期内，由于本公司仅从事电信相关业务，因此本公司整体作为一个经营分部。由于本公司绝大部分经营业务于中国内地进行，所以没有列示地区数据。

(22) 重要会计估计和判断

编制财务报表时，本公司管理层需要运用估计和假设，这些估计和假设会对会计政策的应用及资产、负债、收入及费用的金额产生影响。实际情况可能与这些估计不同。本公司管理层对估计涉及的关键假设和不确定因素的判断进行持续评估，会计估计变更的影响在变更当期和未来期间予以确认。

(a) 应收账款预期信用损失

应收账款预期信用损失基于违约风险和预期信用损失率相关假设确定。本公司在每个资产负债表日对这些假设作出评估，并基于本公司历史信用损失经验、当前市场状况及前瞻性信息选取计算预期信用损失的参数。本公司定期监控并复核与预期信用损失计算相关的假设，包括消费者物价指数、生产价格指数和国内生产总值等宏观经济因素的预期变化。

(b) 固定资产的折旧

本公司固定资产的折旧采用年限平均法并按其入账价值减去预计净残值和减值准备(如有)后在预计使用寿命内计提。本公司每年审阅相关资产的预期使用寿命和净残值，以确定应计入相关报告期的折旧金额。资产的预计使用寿命是本公司根据对同类资产的以往经验并考虑预期的技术改变而确定。如果以前的估计发生重大变化，则会在未来期间对折旧费用进行调整。

(c) 所得税

本公司须缴纳企业所得税。在正常的经营活动中，部分交易和事项的最终税务处理都存在不确定性。在计提各个地区的所得税费用时，本公司需要作出重大判断。如果这些税务事项的最终认定结果与最初入账的金额存在差异，该差异将对作出上述最终认定期间的所得税费用和递延所得税的金额产生影响。

公共资源交易平台仅供标专用
AE2C19C[illegible]1646E1A[illegible]9C88EA14DB9

对于产生递延所得税资产的暂时性差异等，本公司评估了暂时性差异转回的可能性。根据本公司的估计和假设，暂时性差异将在可预见的将来从持续经营所产生的应纳税所得额中转回，即确认递延所得税资产。如果实际情况与估计存在差异，可能导致对递延所得税资产的账面价值进行调整。

(d) 固定资产、无形资产、使用权资产和对联营企业长期股权投资的减值评估

本公司的固定资产、无形资产、使用权资产和对联营企业长期股权投资是本公司总资产的重要组成部分。技术或行业环境的变化均可能令固定资产及无形资产的预计可使用年限或价值出现变动。本公司每年最少对固定资产、使用寿命有限的无形资产、使用权资产和对联营企业长期股权投资进行一次减值审阅以确定是否存在减值迹象。

如某些事件或情况变化显示这些资产的账面金额可能无法收回时，便估计资产的可收回金额。此外，对于无既定可使用期限的无形资产，无论是否出现减值迹象，本公司每年均会估计其可收回金额。

可收回金额是资产 (或资产组) 的公允价值减去处置费用后的净额与资产 (或资产组) 预计未来现金流量的现值两者之间的较高者。在评估预计未来现金流量的现值时，预计未来现金流量会按照能反映当时市场对货币时间价值和资产特定风险评估的税前折现率折现至其现值。在计算预计未来现金流量时，需对收入水平和经营成本作出重大的判断。本公司会运用一切现有资料来确定可收回金额的合理参数，包括按照合理并有依据的假设和对收入和经营成本所作预测得出的估计数额。如果这些估计数额出现变动，可能影响资产的可收回金额，还可能导致计提额外的减值准备。

4 会计政策与会计估计变更

(1) 会计政策变更的内容及原因

本公司于 2022 年度执行了财政部于近年颁布的企业会计准则相关规定及指引，主要包括：

- 《企业会计准则解释第15号》(财会 [2021] 35号) (“解释第15号”) 中“关于企业将固定资产达到预定可使用状态前或者研发过程中产出的产品或副产品对外销售的会计处理”(“试运行销售的会计处理”) 的规定；及
- 解释第15号中“关于亏损合同的判断”的规定；

采用上述规定未对本公司的财务状况及经营成果产生重大影响。

公共资源交易平台专用
AE2C19CE0A7C8E1A02A8BC88EA14DB9

5 税项

(1) 本公司适用的主要税种及其税率列示如下：

税种	计缴标准
增值税	按税法规定计算的销售货物和应税劳务收入的 13%，9%，6%、5%及 3%计算销项税额，在扣除当期允许抵扣的进项税额后，差额部分为应缴增值税
城市维护建设税	当期缴纳的增值税的 7%
教育费附加	当期缴纳的增值税的 3%
地方教育费附加	当期缴纳的增值税 2%

(2) 所得税

根据《中华人民共和国企业所得税法》（“企业所得税法”）及其实施条例，本公司 2022 年度及 2021 年度适用的企业所得税法定税率为 25%。

(3) 增值税

一般计税方法下，应纳增值税额为销项税额扣减可抵扣进项税后的余额，销项税额为根据相关税法规定计算的销售额的 6%、9%和 13%。

根据《中华人民共和国增值税暂行条例》、《财政部 国家税务总局关于将电信业纳入营业税改征增值税试点的通知》(财税〔2014〕43 号)、《财政部 国家税务总局关于全面推开营业税改征增值税试点的通知》(财税〔2016〕36 号) 及《财政部 税务总局 海关总署关于深化增值税改革有关政策的公告》(财政部 税务总局 海关总署公告 2019 年第 39 号)，本公司增值电信服务及信息技术服务、技术咨询服务等现代服务业的业务适用的增值税税率为 6%，基础电信服务适用的增值税税率为 9%，通信终端销售等业务适用的增值税税率为 13%。

(4) 税收优惠

(a) 根据《财政部 税务总局 海关总署关于深化增值税改革有关政策的公告》(财政部 税务总局 海关总署公告 2019 年第 39 号) 以及《国家发展改革委等部门印发 <关于促进服务业领域困难行业恢复发展的若干政策> 的通知》(发改财金〔2022〕271 号) 的相关规定，本公司作为电信服务企业，自 2019 年 4 月 1 日至 2022 年 12 月 31 日，可按照当期可抵扣进项税额加计 10%，抵减增值税应纳税额。

公共资源交易平台投标专用
AE2C19CE-[illegible]-5CE1A62[illegible]-9EA14DB9

(b) 根据《财政部 税务总局关于延长部分税收优惠政策执行期限的公告》(2021 年第 6 号) 及《财政部 税务总局 科技部关于提高研究开发费用税前加计扣除比例的通知》(财税〔2018〕99 号)，于 2023 年 12 月 31 日前，企业开展研发活动中实际发生的研发费用，未形成无形资产计入当期损益的，在按规定据实扣除的基础上，再按照实际发生额的 75%在税前加计扣除；形成无形资产的，按照无形资产成本的 175%在税前摊销。

(5) 应交税费

	2022 年	2021 年
应交企业所得税	2,054,059,160.12	1,821,669,387.41
代扣个人所得税	76,135,615.94	71,811,584.44
其他	21,279,621.63	20,457,863.16
合计	2,151,474,397.69	1,913,938,835.01

6 货币资金

	注	2022 年	2021 年
现金及银行活期存款	(i)	2,077,438,012.00	3,253,603,719.59
其他货币资金		14,469,745.12	6,659,787.59
现金及现金等价物小计		2,091,907,757.12	3,260,263,507.18
三个月以上银行定期存款		440,590,000.00	1,350,590,000.00
应收利息		43,130,843.27	13,641,221.38
使用受限制的货币资金	(ii)	7,668,296.16	11,632,957.10
合计		2,583,296,896.55	4,636,127,685.66

(i) 于 2022 年 12 月 31 日，本公司银行存款包括存放于中国移动通信公司财务有限公司（“财务公司”）的款项人民币 560,189,368.30 元 (2021 年 12 月 31 日：人民币 1,777,433,804.85 元)，均为活期存款。

(ii) 本公司使用受限制的货币资金主要为诉讼冻结款。

公共资源交易平台 仅供投标专用
AE2C19CEC77646E1A6218B

7 应收账款

(1) 应收账款按客户类别分析如下：

	附注	2022 年	2021 年
应收用户欠费		1,563,052,200.68	2,226,013,910.73
应收关联公司		1,492,738,989.47	851,970,960.14
应收非关联公司		25,453,384.38	39,213,353.13
小计		4,081,244,574.53	3,117,198,224.00
减：坏账准备		(976,384,419.39)	(955,864,027.87)
合计		3,104,860,155.14	2,161,334,196.13

(2) 应收账款按账龄分析如下：

	2022 年	2021 年
1 年以内 (含 1 年)	3,178,705,713.39	2,273,661,523.50
1 年至 2 年 (含 2 年)	488,705,447.24	406,674,666.71
2 年至 3 年 (含 3 年)	192,754,809.99	159,837,945.74
3 年以上	221,078,603.91	277,024,088.05
小计	4,081,244,574.53	3,117,198,224.00
减：坏账准备	(976,384,419.39)	(955,864,027.87)
合计	3,104,860,155.14	2,161,334,196.13

账龄自应收账款确认日起开始计算。

(3) 应收账款预期信用损失的评估：

本公司根据信用风险特征，将应收账款分为个人用户、公司用户、低风险金融资产和其他四类，并采用简化方法计量预期信用损失，即以整个存续期预期信用损失的金额计提应收账款的坏账准备。其中，个人用户、公司用户具有相似信用风险特征，采用组合方式计提坏账准备。低风险金融资产，主要为中国移动公司内部各成员单位之间形成的应收款项、与其他电信运营商结算款、历史上从未发生过坏账损失且信用级别较高的大型公司用户应收款项以及其他一些风险极低的金融资产。除上述分类外的应收账款划分为其他类别的金融资产。

公共资源交易平台 仅供查验专用
AE2C19CEC7

(a) 个人用户

	2022 年 12 月 31 日			2021 年 12 月 31 日		
	预期信用损失率	年末账面余额	年末坏账准备	预期信用损失率	年末账面余额	年末坏账准备
账龄 1 至 30 日	2.0%	281,534,660.40	5,630,693.21	2.0%	238,433,389.10	4,768,665.81
账龄 31 至 90 日	20.0%	45,758,570.33	9,151,714.07	20.0%	63,458,546.47	12,691,709.32
账龄 91 至 1 年	80.0%	128,807,130.18	103,045,704.14	80.0%	126,093,169.77	100,874,551.80
账龄超过 1 年	100.0%	44,500,046.98	44,500,046.98	100.0%	32,557,453.20	32,557,453.20
合计		500,600,407.89	162,328,158.40		459,542,478.54	150,892,380.13

(b) 政企用户

	2022 年 12 月 31 日			2021 年 12 月 31 日		
	预期信用损失率	年末账面余额	年末坏账准备	预期信用损失率	年末账面余额	年末坏账准备
账龄 1 至 180 日	3.0%	647,967,170.99	19,439,015.13	3.0%	407,298,183.63	12,218,958.38
账龄 180 日至 1 年	25.0%	585,410,990.52	146,352,747.63	25.0%	550,135,906.15	137,544,960.01
账龄 1 至 2 年	65.0%	446,352,363.81	290,129,036.47	65.0%	374,534,698.52	243,447,554.01
账龄 2 至 3 年	85.0%	177,439,339.62	150,823,438.68	85.0%	159,742,581.84	135,781,194.59
账龄超过 3 年	100%	205,281,927.85	205,281,927.85	100%	274,759,602.05	274,759,602.05
合计		2,062,451,792.79	812,026,165.76		1,766,471,432.19	803,752,269.04

公共资源交易电子交易标专用
AE2919BC7646F1F62A8BC88EA14DB9

(c) 低风险金融资产

该部分 2022 年 12 月 31 日账面余额为人民币 512,219,463.32 元 (2021 年 12 月 31 日: 人民币 870,339,781.08 元), 2022 年 12 月 31 日坏账准备为人民币 194,804.74 元 (2021 年 12 月 31 日: 人民币 184,081.21 元)。

(4) 坏账准备变动情况如下:

	2022 年	2021 年
年初余额	955,864,027.87	737,640,808.29
本年计提和转回	176,174,972.60	336,146,251.68
本年收回与核销	(155,654,581.08)	(117,923,032.10)
年末余额	976,384,419.39	955,864,027.87

8 应收资金集中管理款

本公司通过银行参与了母公司中国移动通信有限公司 (“中移通信”) 的资金集中管理计划。根据相关资金结算协议, 该资金存放于指定银行账户且本公司可以不受任何限制地使用该等资金, 并按照约定从银行收取利息。

9 其他应收款

(1) 其他应收款分类分析如下:

	2022 年	2021 年
押金或保证金	27,759,942.58	25,447,620.28
进项税	84,765,227.82	64,076,418.34
其他	18,523,536.12	1,812,562.18
小计	131,048,706.52	91,336,600.80
减: 坏账准备	(131,587.00)	(151,587.00)
合计	130,917,119.52	91,185,013.80

公共资源交易平台投标专用
AE2C19CEC7764E1AC1BC98EA14DB9

(2) 按账龄分析如下：

	2022 年	2021 年
1 年以内 (含 1 年)	128,755,161.64	88,930,619.57
1 年至 2 年 (含 2 年)	490,635.00	487,425.88
2 年至 3 年 (含 3 年)	160,930.88	1,786,968.35
3 年以上	1,641,979.00	131,587.00
小计	131,048,706.52	91,336,600.80
减：坏账准备	(131,587.00)	(151,587.00)
合计	130,917,119.52	91,185,013.80

账龄自其他应收款确认日起开始计算。

(3) 坏账准备变动情况如下：

	2022 年	2021 年
年初余额	151,587.00	131,587.00
本年计提	-	20,000.00
本年转回	(20,000.00)	-
年末余额	131,587.00	151,587.00

10 存货

(1) 本公司按存货类别分析如下：

	2022 年	2021 年
库存商品	174,238,154.30	295,170,472.27
原材料及备品备件	10,769,859.32	10,205,191.52
小计	185,008,013.62	305,375,663.79
减：存货跌价准备	(6,320,038.11)	(18,857,806.71)
合计	178,687,975.51	286,517,857.08

本公司存货跌价准备分析如下：

	2022 年 1 月 1 日余额	本年计提	本年转销	2022 年 12 月 31 日余额
库存商品	(18,857,806.71)	(5,853,086.88)	18,390,855.48	(6,320,038.11)
合计	(18,857,806.71)	(5,853,086.88)	18,390,855.48	(6,320,038.11)

本公司无用于担保的存货 (2021 年：无)。

公共资源交易平台技术专用
AE2C19CEC7646E1A6B5C88EA14DB9

11 合同资产

	2022 年 12 月 31 日	2021 年 12 月 31 日
合同资产	473,021,396.63	116,565,749.68
减：减值准备	(16,080,054.26)	(4,288,345.73)
减：列示于其他非流动资产的合	(29,185,127.29)	(14,572,935.38)
合计	427,756,215.08	97,704,468.57

于 2022 年 12 月 31 日及 2021 年 12 月 31 日，本公司合同资产均按组合计提减值准备，合同资产的预期损失率在 3%至 5%之间。

12 其他流动资产

	2022 年	2021 年
预缴增值税	106,567,644.30	833,406,210.20
待认证进项税额	11,162,812.68	2,082,895.18
其他	29,434,441.16	859,065.67
合计	147,164,898.14	836,348,171.05

13 长期股权投资

	2022 年	2021 年
联营企业	79,565,420.07	78,803,096.25
减：减值准备	-	-
合计	79,565,420.07	78,803,096.25

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88A14DB9

本公司联营公司正数网络技术有限公司（以下简称“正数公司”）成立于 2020 年 8 月 3 日，注册地河南省郑州市。正数公司注册资本 10 亿元，本公司认缴出资比例为 30%，豫信电子科技集团有限公司认缴出资比例为 30%，河南日报报业集团有限公司认缴出资比例 21%，建信金融科技（河南）有限公司认缴出资比例 19%。根据公司章程约定，股东按照认缴出资比例行使表决权，按实缴的出资比例分[illegible]。截止 2022 年 12 月 31 日，本公司联营企业正数公司各股东均未全额出资，本公司实际[illegible]比为 45.45%。

正数公司主要提供系统管理、应用开发、数据融合、安全机制等专业化综合服务。

正数公司董事会 7 名董事中的 1 名由本公司任命，总经理也由本公司任命，可以通过以上代表参与正数公司财务和经营政策的制定，本公司能够对正数公司施加重大影响，故将其作为联营企业核算。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

(a) 本公司的联营企业的基本情况如下：

企业名称	主要经营地	注册地	注册资本	持股比例	业务性质	对本公司活动是否具有战略性
正数网络技术有限公司	河南省郑州市	河南省郑州市	10 亿元	3[illegible]%	主要提供系统管理、应用开发、数据库、合作、安全机制等专业化综合服务。	否

公共资源交易平台投标专用
AE2619B6776461A62A8BC88EA14DB9

14 固定资产

	注	2022 年	2021 年
固定资产	(a)	36,334,289,863.98	36,334,289,863.98
固定资产清理		38,643,141.86	41,438,191.45
合计		36,372,933,005.84	36,375,728,055.43

(a) 固定资产

	房屋及建筑物	通信设备	办公设备及其他	合计
原值				
2021 年 1 月 1 日余额	6,789,301,739.70	83,635,312,598.82	820,130,786.15	91,244,745,124.67
在建工程转入	205,589,258.55	8,662,632,975.23	51,965,049.74	8,920,187,283.52
本年减少	(7,547,089.38)	(1,986,316,185.99)	(52,334,839.17)	(2,046,198,114.54)
2021 年 12 月 31 日余额	6,987,343,908.87	90,311,629,388.06	819,760,996.72	98,118,734,293.65
在建工程转入	388,188,704.78	8,563,305,190.35	19,816,744.89	8,971,310,640.02
本年减少	(4,990,383.19)	(1,024,807,831.44)	(31,410,964.62)	(1,061,209,179.25)
2022 年 12 月 31 日余额	7,370,542,230.46	97,850,126,746.97	808,166,776.99	106,028,835,754.42
减：累计折旧				
2021 年 1 月 1 日余额	(2,694,353,768.08)	(53,145,397,106.57)	(700,247,631.96)	(56,539,998,506.61)
本年计提折旧	(229,379,892.12)	(7,337,733,421.54)	(40,550,771.99)	(7,607,664,085.65)
折旧冲销	6,428,825.10	1,634,715,969.54	49,035,614.14	1,690,180,408.78
2021 年 12 月 31 日余额	(2,917,304,835.10)	(58,848,414,558.57)	(691,762,789.81)	(62,457,482,183.48)
本年计提折旧	(228,792,290.61)	(7,515,855,011.45)	(33,533,721.05)	(7,778,181,023.11)
折旧冲销	4,164,115.72	986,437,310.29	30,308,890.18	1,020,910,316.19
2022 年 12 月 31 日余额	(3,141,933,009.99)	(65,377,832,259.73)	(694,987,620.68)	(69,214,752,890.40)
减：减值准备				
2021 年 1 月 1 日余额	-	(536,393,150.01)	(672,244.94)	(537,065,394.95)
处置转销	-	41,679,167.72	672,244.94	42,351,412.66
2021 年 12 月 31 日余额	-	(494,713,982.29)	-	(494,713,982.29)
处置转销	-	14,920,982.25	-	14,920,982.25
2022 年 12 月 31 日余额	-	(479,793,000.04)	-	(479,793,000.04)
账面价值				
2022 年 12 月 31 日	4,228,609,220.47	31,992,501,487.20	113,179,156.31	36,334,289,863.98
2021 年 12 月 31 日	4,070,039,073.77	30,968,500,847.20	127,998,206.91	35,166,538,127.88

于 2022 年 12 月 31 日及 2021 年 12 月 31 日，本公司无抵押或融资租入的固定资产，亦无重大闲置的固定资产。

公共资源交易平台 联盟专用
AE2C19CE0776-4211-A8BC-A14DB9

15 在建工程

	2022 年	2021 年
在建工程	3,487,096,364.04	3,455,624,524.50
工程物资	451,958,693.50	472,624,376.05
合计	3,939,055,057.54	3,928,248,900.55

(1) 在建工程

	本公司
成本	
2021 年 12 月 31 日余额	3,455,624,524.50
本年增加	9,142,030,061.26
本年转入固定资产	(8,971,310,640.02)
本年转入无形资产	(139,247,581.70)
2022 年 12 月 31 日余额	3,487,096,364.04
减：减值准备	
2021 年 12 月 31 日余额	-
2022 年 12 月 31 日余额	-
账面价值	
2022 年 12 月 31 日	3,487,096,364.04
2021 年 12 月 31 日	3,455,624,524.50

本公司认为在建工程的账面价值已充分反映可收回金额，无需计提减值准备。

(2) 工程物资

	2022 年	2021 年
工程材料及设备	451,958,693.50	472,624,376.05
减：减值准备	-	-
合计	451,958,693.50	472,624,376.05

公共资源交易平台技术专用
AE2C19CEC77646E1A62A8DC88A14DB9

16 使用权资产

本公司作为承租人的租赁情况如下：

	铁塔及相关配套设备	房屋及建筑物	其他	合计
原值				
2021 年 1 月 1 日余额	297,802.82	1,999,0[illegible]5,470.29	532,426,032.39	7,150,789,305.50
本年增加	323,[illegible]54,131.79	321,[illegible]27,763.20	98,673,345.30	743,955,240.23
本年减少	(97,200,897.97)	(332,[illegible]35,211.13)	(121,382,162.24)	(550,618,271.34)
2021 年 12 月 31 日余额	4,845,451,036.58	1,9[illegible]8,958,022.36	509,717,215.45	7,344,126,274.39
本年增加	3,962,508,169.48	507,207,908.36	397,394,758.58	4,867,110,836.42
本年减少	(186,787,370.85)	(460,127,961.47)	(152,051,118.56)	(798,966,450.68)
2022 年 12 月 31 日余额	[illegible]7,835.41	2,036,037,969.25	755,060,855.47	11,412,270,660.13
减：累计折旧				
2021 年 1 月 1 日余额	(2,511,778,988.68)	(1,107,836,263.20)	(337,758,944.05)	(3,957,374,195.93)
本年增加	(926,216,874.82)	(379,754,832.95)	(104,248,536.53)	(1,410,220,244.30)
本年减少	37,216,114.76	265,705,084.59	114,905,401.64	417,826,600.99
2021 年 12 月 31 日余额	(3,400,779,748.74)	(1,221,886,011.56)	(327,102,078.94)	(4,949,767,839.24)
本年增加	(958,758,910.22)	(389,460,456.76)	(174,269,896.43)	(1,522,489,263.41)
本年减少	140,036,790.98	413,825,295.29	136,254,706.79	690,116,793.06
2022 年 12 月 31 日余额	(4,219,501,867.98)	(1,197,521,173.03)	(365,117,268.58)	(5,782,140,309.59)
账面价值				
2022 年 12 月 31 日	4,401,669,967.43	838,516,796.22	389,943,586.89	5,630,130,350.54
2021 年 12 月 31 日	1,444,671,287.84	767,072,010.80	182,615,136.51	2,394,358,435.15

公共资源交易平台登录专用
AE2619CEC77646E1A62A8BC88EA14DB9

17 无形资产

	土地使用权	软件	合计
原值			
2021 年 1 月 1 日余额	1,026,675,656.00	2,188,427,731.91	3,215,103,387.91
本年增加金额	1,542,749.02	608,783,643.55	610,326,392.57
本年减少金额	-	-	-
2021 年 12 月 31 日余额	1,028,218,405.02	2,797,211,375.46	3,825,429,780.48
本年增加金额	10,684,506.94	361,202,526.95	371,887,033.89
本年减少金额	-	-	-
2022 年 12 月 31 日余额	1,038,902,911.96	3,158,413,902.41	4,197,316,814.37
减：累计摊销			
2021 年 1 月 1 日余额	(239,640,221.92)	(1,491,566,877.06)	(1,731,207,098.98)
本年增加金额	(23,345,310.89)	(260,833,086.85)	(284,178,397.74)
本年减少金额	-	-	-
2021 年 12 月 31 日余额	(262,985,532.81)	(1,752,399,963.91)	(2,015,385,496.72)
本年增加金额	(22,971,428.53)	(329,138,475.24)	(352,109,903.77)
本年减少金额	-	-	-
2022 年 12 月 31 日余额	(285,956,961.34)	(2,081,538,439.15)	(2,367,495,400.49)
账面价值			
2022 年 12 月 31 日	752,945,950.62	1,076,875,463.26	1,829,821,413.88
2021 年 12 月 31 日	765,232,872.21	1,044,811,411.55	1,810,044,283.76

于 2022 年 12 月 31 日及 2021 年 12 月 31 日，本公司无用于抵押和担保的无形资产。

本公司认为无形资产的账面价值已充分反映可收回金额，无需计提减值准备。

公共资源交易平台使用专用
AE2C19CEC77646E1A62A8BC88EA14DB9

18 长期待摊费用

	2022 年	2021 年
预付服务费	617,201,971.43	565,822,757.38
租入资产改良支出	33,962,176.37	36,512,333.68
其他	96,215,128.93	59,158,771.44
合计	747,379,276.73	661,493,862.50

19 递延所得税资产及负债

(1) 未经抵消的递延所得税资产：

	递延所得税资产		
	年初余额	本年增减计入损益	年末余额
坏账准备	239,046,402.48	5,115,099.13	244,161,501.61
合同资产减值准备	1,072,086.44	2,947,927.13	4,020,013.57
存货跌价准备	4,714,451.68	(3,134,442.15)	1,580,009.53
固定资产减值准备	123,678,495.57	(3,730,245.56)	119,948,250.01
处置固定资产/无形资产损失	59,550,172.41	(19,490,288.26)	40,059,884.15
固定资产折旧	129,447,662.41	16,029,027.43	145,476,689.84
无形资产摊销	218,188.36	(68,179.71)	150,008.65
递延收益（仅积分递延和金币递延）	447,936,637.09	(21,755,976.65)	426,180,660.44
递延收益（除积分与金币外递延收益）	70,101,512.84	7,929,431.03	78,030,943.87
房屋装修费	955,737.05	(256,224.40)	699,512.65
职工教育经费/工会经费	60,941,780.84	(4,692,914.75)	56,248,866.09
其他预计费用	799,024,985.70	159,972,533.82	958,997,519.52
新租赁准则	48,305,663.19	(20,091,552.26)	28,214,110.93
其他	6,270,291.10	4,368,474.49	10,638,765.59
合计	1,991,264,067.16	123,142,669.29	2,114,406,736.45

(2) 未经抵消的递延所得税负债：

	递延所得税负债		
	年初余额	本年增减计入损益	年末余额
利息收入	(68,222,814.37)	(106,736,729.79)	(174,959,544.16)
合计	(68,222,814.37)	(106,736,729.79)	(174,959,544.16)

公共资源交易平台数据专用

(3) 于资产负债表日，列示在资产负债表中的递延所得税资产和负债净额：

	2022 年	2021 年
递延所得税资产	1,939,447,192.29	1,923,041,252.79

20 其他非流动资产

	2022 年	2021 年
合同成本	1,241,494,895.62	893,547,468.97
合同资产	30,721,186.62	15,339,232.68
预付工程款	13,303,698.42	21,967,998.13
一年以上定期存款及大额存单	900,000,000.00	-
其他	628,336,105.66	-
减：合同资产减值准备	(1,536,059.33)	(766,297.30)
合计	2,812,319,826.99	930,088,402.48

2022年度，合同履约成本摊销计入营业成本的金额为人民币1,344,670,058.09元(2021年度：人民币 868,415,083.34 元)。

21 应付票据

	2022 年	2021 年
银行承兑汇票	1,395,309,408.42	1,082,158,904.26
商业承兑汇票	1,741,576,280.18	1,527,521,324.67
合计	3,136,885,688.60	2,609,680,228.93

22 应付账款

	2022 年	2021 年
应付关联公司	5,640,272,025.47	5,326,580,555.80
应付非关联公司工程款	3,927,981,881.83	4,826,524,223.57
应付非关联公司其他款	5,026,994,363.09	4,558,569,767.20
合计	14,595,248,270.39	14,711,674,546.57

公共资源交易平台技术专用
AE2C19CEC7F546E1A62A8D

23 预收账款

	2022 年	2021 年
1 年以内 (含 1 年)	4,024,161,161.19	6,428,559,468.49

于 2022 年 12 月 31 日及 2021 年 12 月 31 日，均无账龄超过一年的单项重大预收款项。

24 合同负债

	2022 年	2021 年
未兑换的积分计划	1,704,722,650.86	1,791,746,557.47
未使用的递延流量	299,200,433.48	188,552,045.87
与合同相关的预存款	665,806,657.08	751,295,898.81
合计	2,669,729,741.42	2,731,594,502.15

合同负债将在服务提供时确认为营业收入。于 2021 年 12 月 31 日合同负债中大部分已在一年内于合并利润表确认为营业收入。

25 应付职工薪酬

	2022 年	2021 年
短期薪酬	257,718,878.61	254,597,249.81
离职后福利	2,430,000.00	1,810,000.00
合计	260,148,878.61	256,407,249.81

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC

(1) 短期薪酬

	2022 年 1 月 1 日余额	本年发生额	本年支付额	2022 年 12 月 31 日余额
工资、奖金、津贴和补贴		2,719,733,654.72	2,719,733,654.72	-
职工福利费		100,920,389.72	100,920,389.72	-
社会保险费		223,529,426.46	223,529,426.46	-
- 医疗保险费		212,818,888.62	212,818,888.62	-
- 工伤保险费		6,921,661.13	6,921,661.13	-
- 生育保险费		3,788,876.71	3,788,876.71	-
住房公积金		262,025,663.01	262,025,663.01	-
非货币性福利	-	5,098,951.55	5,098,951.55	-
工会经费	10,731,600.08	54,394,673.05	54,831,559.17	10,294,713.96
职工教育经费	243,217,123.33	977,486.22	19,749,145.18	224,995,464.37
劳动保护费	98,526.40	35,861,599.34	13,531,425.46	22,428,700.28
劳务费	-	695,442,415.30	695,442,415.30	-
合计	254,597,249.81	4,097,984,259.37	4,094,862,630.57	257,718,878.61

	2021 年 1 月 1 日余额	本年发生额	本年支付额	2021 年 12 月 31 日余额
工资、奖金、津贴和补贴	-	2,641,468,077.07	2,641,468,077.07	-
职工福利费	-	98,539,319.56	98,539,319.56	-
社会保险费	-	205,564,477.81	205,564,477.81	-
- 医疗保险费	-	194,957,235.07	194,957,235.07	-
- 工伤保险费	-	7,225,808.07	7,225,808.07	-
- 生育保险费	-	3,381,434.67	3,381,434.67	-
住房公积金	-	239,944,757.29	239,944,757.29	-
非货币性福利	-	2,592,403.98	2,592,403.98	-
工会经费	11,388,950.73	52,901,596.62	53,558,947.27	10,731,600.08
职工教育经费	164,431,943.79	105,690,685.25	26,355,505.71	243,767,123.33
劳动保护费	2,627,858.33	5,743,013.29	8,272,345.22	98,526.40
劳务费	-	671,769,529.18	671,769,529.18	-
合计	178,448,752.85	4,024,213,860.05	3,948,065,363.09	254,597,249.81

公共资源交易平台电子证书专用
AE2C19CEC77646E1A62[illegible]8EA14DB9

(2) 设定提存计划

	2022 年 1 月 1 日余额	本年发生额	本年支付额	2022 年 12 月 31 日余额
基本养老保险费	-	339,657,815.15	339,657,815.15	-
失业保险费	-	14,955,430.36	14,955,430.36	-
年金	-	206,583,699.43	206,583,699.43	-
合计	-	561,196,944.94	561,196,944.94	-

	2021 年 1 月 1 日余额	本年发生额	本年支付额	2021 年 12 月 31 日余额
基本养老保险费	-	310,449,204.41	310,449,204.41	-
失业保险费	-	14,343,726.44	14,343,726.44	-
年金	-	194,825,162.43	194,825,162.43	-
合计	-	519,618,093.28	519,618,093.28	-

(3) 辞退福利

	2022 年	2021 年
应付离退休后补充福利（流动部分）	2,430,000.00	1,810,000.00

26 其他应付款

	2022 年	2021 年
应付押金或保证金	384,393,223.09	436,440,067.67
应付代收代付款及暂收款	35,726,864.04	22,051,651.80
应付职工垫付款项	12,228,171.92	12,481,184.30
其他	86,557,064.50	87,771,749.72
合计	518,905,323.55	558,744,653.49

账龄分析：

	2022 年	2021 年
1 年以内 (含 1 年)	463,070,600.89	500,177,653.25
1 年至 2 年 (含 2 年)	6,349,148.22	7,208,822.93
2 年至 3 年 (含 3 年)	5,718,680.69	6,492,990.09
3 年以上	43,766,893.75	44,865,187.22
合计	518,905,323.55	558,744,653.49

公共资源交易平台技术专用
AE2C19CE07646E1A62A6C0DA14DB9

本公司其他应付款主要为押金及保证金、代收代付款及暂收款。本公司无 1 年以上单项重大其他应付款。

27 一年内到期的非流动负债

	附注	2022 年	2021 年
租赁负债	28	1,581,725,815.31	1,306,312,858.53

28 租赁负债

	附注	2022 年	2021 年
租赁负债		5,629,061,625.32	2,423,156,200.29
减：一年内到期的租赁负债	27	(1,581,725,815.31)	(1,306,312,858.53)
合计		4,047,335,810.01	1,116,843,341.76

本公司未纳入租赁负债，但将导致未来潜在现金流出的事项包括：

2022 年度本公司将不属于与指数和利率相关的可变租金在发生时直接计入当期损益，金额为人民币 443,926,132.18 元 (2021 年度：人民币 557,521,267.43 元)。

29 递延收益

	2022 年	2021 年
政府补助	310,555,268.08	278,843,969.34
- 与资产相关	273,195,792.43	238,560,246.06
- 与收益相关	37,359,475.65	40,283,723.28
合计	310,555,268.08	278,843,969.34

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8B

(1) 涉及政府补助的项目

2022 年

	年初余额	本年新增政府补助	本年计入其他收益金额	本年计入营业外收入金额	年末余额
电信普遍服务	139,481,589.51	77,000.00	(27,520,735.46)	-	112,037,854.05
土地出让及拆迁补偿	73,262,552.10	946,330.28	(2,686,033.41)	-	71,522,848.97
其他政府补助	66,099,827.73	111,115,811.36	(50,190,513.81)	(30,060.22)	126,994,565.06
合计	278,843,969.34	112,139,141.64	(80,397,282.68)	(30,060.22)	310,555,268.08

2021 年

	年初余额	本年新增政府补助	本年计入其他收益金额	本年计入营业外收入金额	年末余额
电信普遍服务	183,825,795.29	7,472,800.00	(51,817,005.78)	-	139,481,589.51
土地出让及拆迁补偿	74,571,991.44	3,741,115.46	(5,050,554.80)	-	73,262,552.10
其他政府补助	5,213,588.64	71,699,967.60	(10,742,531.51)	(71,197.00)	66,099,827.73
合计	263,611,375.37	82,913,883.06	(67,610,092.09)	(71,197.00)	278,843,969.34

30 实收资本

本公司于 12 月 31 日的注册资本结构如下：

	2022 年		2021 年	
	金额	%	金额	%
	人民币		人民币	
中国移动通信有限公司	4,367,733,640.58	100.00	4,367,733,640.58	100.00

31 资本公积

	2022 年 1 月 1 日余额	本年增加	本年减少	2022 年 12 月 31 日余额
资本溢价	-	1,823,536,074.45	-	1,823,536,074.45
股份支付	264,288,061.15	15,269,287.89	-	279,557,349.04
其他	1,833,064.64	-	-	1,833,064.64
合计	266,121,125.79	1,838,805,362.34	-	2,104,926,488.13

	2021 年 1 月 1 日余额	本年增加	本年减少	2021 年 12 月 31 日余额
股份支付	248,240,359.90	16,047,701.25	-	264,288,061.15
其他	1,833,064.64	-	-	1,833,064.64
合计	250,073,424.54	16,047,701.25	-	266,121,125.79

公共资源交易平台投标专用
AE2C19CEC7764E1C18BC88EA14DB9

注：

1）截至 2022 年 12 月 31 日，本公司今年收到本公司之母公司中移通信以注资计入资本公积的形式拨付的募集资金款项 1,823,536,074.45 元，用于本公司开展的“5G 精品网络建设项目”、“千兆智家建设项目”和“智慧中台建设项目”。相关款项已存放于本公司募集资金专户。

2）本公司母公司之间接控股公司中国移动有限公司以其自身股份直接授予本公司部分员工股份期权，于股份期权生效条件满足后，由中国移动有限公司向其进行股份的支付和结算。中国移动有限公司将此项以自身权益结算的股份支付作为对本公司的投资增加，并按照股份期权授予日公允价值确认的期权费用下推至本公司。截至 2022 年 12 月 31 日，中国移动有限公司累计向本公司下推的期权费用总额为人民币 279,557,349.04 元。

32 其他综合收益

	资产负债表中其他综合收益			2022 年度利润表中其他综合收益			
	2021 年 12 月 31 日	税后归属于母公司	2022 年 12 月 31 日	所得税前发生额	减：其他综合收益本年转出	减：所得税费用	税后归属于母公司
不能重分类进损益的其他综合收益							
重新计量设定受益计划变动额	(1,490,000.00)	788,848.78	(701,151.22)	788,848.78	-	-	788,848.78
合计	(1,490,000.00)	788,848.78	(701,151.22)	788,848.78	-	-	788,848.78

33 盈余公积

	2022 年 12 月 31 日	2021 年 12 月 31 日
法定盈余公积	7,730,890,058.83	7,730,890,058.83
任意盈余公积	8,314,771,380.50	8,314,771,380.50
合计	16,045,661,439.33	16,045,661,439.33

34 利润分配及年末未分配利润

(a) 提取各项盈余公积

根据《中华人民共和国公司法》及本公司《公司章程》，本公司按年度净利润的 10%提取法定盈余公积金，按年度净利润的 10%提取任意盈余公积金。当法定盈余公积金累计额达到注册资本的 50%以上时，可不再提取。

(b) 向投资者分配现金利润

本公司于 2022 年向投资者分配利润共人民币 6,863,907,654.22 元 (2021 年：人民币 1,549,147,475.46 元)。

公共资源交易平台技术专用

35 营业收入

(1) 营业收入

	2022 年	2021 年
主营业务收入	41,113,314,969.64	41,809,200,314.48
其他业务收入	917,656,377.86	797,375,153.36
合计	42,030,971,347.50	42,606,575,467.84

(2) 营业成本

	2022 年	2021 年
主营业务成本	30,810,616,913.58	28,158,832,369.36
其他业务成本	890,446,800.67	697,839,609.62
合计	31,701,063,714.25	28,856,671,978.98

本公司营业收入主要为与客户之间的合同产生的收入，其余营业收入金额不重大。本公司主营业务收入主要为电信服务收入，其他业务收入主要为销售商品收入。

本公司尚未完成的履约义务主要与通信服务相关。本公司一般按月度或其他固定期限与客户签订服务合同，并根据合同约定按月向客户开具账单以获取无条件的对价收款权。截至年末，大部分分配至剩余履约义务的交易对价预计在提供服务后一年内确认。对于预计期限在一年或更短期限的合同，以及对于按履约义务完成进度即可直接发出账单确认收入和收款权的合同，本公司采用《企业会计准则第 14 号 - 收入》允许的实务简化方法，因此，相关剩余履约义务的信息未予披露。

36 税金及附加

	2022 年	2021 年
城市房地产税	57,647,506.14	56,394,171.85
土地使用税	14,987,601.71	14,851,834.72
印花税	11,157,708.46	10,690,633.55
其他	528,265.31	717,803.05
合计	84,321,081.62	82,654,443.17

公共资源交易平台 投标专用
AE2C19CEC77646E1A62A8BC8...A14DB9

37 财务净收益

	2022 年	2021 年
利息收入	(622,363,348.12)	(491,510,216.80)
利息支出	88,667,132.54	111,699,586.03
其他	2,942,497.49	5,152,553.33
合计	(530,753,718.09)	(374,658,077.44)

38 其他收益

	2022 年	2021 年
政府补助	80,397,282.68	67,610,092.09
代扣个人所得税手续返还	1,788,544.78	1,793,215.43
其他	34,441.64	-
合计	82,220,269.10	69,403,307.52

39 信用减值损失

	2022 年	2021 年
应收账款	176,174,972.60	336,146,251.68
其他应收款	(20,000.00)	20,000.00
合计	176,154,972.60	336,166,251.68

40 营业外收支

(1) 营业外收入

	2022 年	2021 年
违约金或赔偿金	23,488,630.63	11,466,229.38
无法支付的应付款项利得	91,815,595.55	58,587,871.99
非流动资产报废收益	10,951,709.11	6,115,637.11
其他	21,222,552.92	18,038,931.91
合计	147,478,488.21	94,208,670.39

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

(2) 营业外支出

	2022 年	2021 年
非流动资产报废损失	4,226,850.38	282,482,602.09
捐赠支出	4,999,750.86	5,000,000.00
其他支出	14,404,453.81	(10,542,966.29)
合计	23,631,055.05	276,939,635.80

41 所得税费用

(1) 本年所得税费用组成

	2022 年	2021 年
本年所得税	2,536,673,650.98	2,650,877,057.36
递延所得税的变动	(16,405,939.50)	(478,903,221.67)
合计	2,520,267,711.48	2,171,973,835.69

递延所得税费用分析如下：

	2022 年	2021 年
暂时性差异的产生和转回	(16,405,939.50)	(478,903,221.67)

(2) 所得税费用与会计利润的关系如下：

	2022 年	2021 年
税前利润	10,013,453,160.16	8,606,164,561.07
按税率 25%计算的预期所得税	2,503,363,290.04	2,151,541,140.27
不可抵扣的成本费用的税务影响	18,562,269.25	23,897,010.63
汇算清缴差异	(1,657,847.81)	(3,464,315.21)
本年所得税费用	2,520,267,711.48	2,171,973,835.69

公共资源交易平台授权专用
AE2C19CEC77646E1A6[illegible]C88EA14DB9

42 利润表补充资料

对利润表中的费用按性质分类的信息如下：

	2022 年	2021 年
营业收入	46,03[illegible],971,347.50	42,606,575,467.84
减：网络运营及支撑支出	(16,33[illegible],776,303.74)	(14,191,767,739.34)
人工成本及劳务费	(4,88[illegible],736,228.30)	(4,573,139,654.58)
销售产品成本及其他	([illegible],446,800.67)	(697,839,609.62)
折旧费和摊销费用	[illegible],641,816,331.84)	(9,295,111,958.38)
广告、宣传及客户服务费	(1,007,041,626.37)	(910,810,392.52)
社会渠道费用	(1,619,951,061.45)	(1,880,956,363.70)
网间结算支出	(1,161,753,805.09)	(1,120,444,168.21)
财务净收益	530,753,718.09	374,658,077.44
税金及附加	(84,321,081.62)	(82,654,443.17)
其他收益	82,220,269.10	69,403,307.52
投资 (收益) / 损失	762,323.82	(18,208,608.90)
信用减值损失	(176,154,972.60)	(336,166,251.68)
资产减值损失	(19,894,760.53)	(1,859,975.88)
其他	(1,128,208,959.30)	(1,152,782,160.34)
营业利润	9,889,605,727.00	8,788,895,526.48

公共资源交易平台登记专用
AE2619CEC77646E1A62A8BC88EA14DB9

43 现金流量表补充资料

(1) 将净利润调节为经营活动的现金流量：

	2022 年	2021 年
净利润	6,493,185,448.68	6,434,190,725.38
加：资产减值损失	19,894,760.53	1,859,975.88
信用减值损失	176,154,972.60	336,166,251.68
固定资产折旧	7,778,181,023.11	7,607,664,085.65
使用权资产折旧	1,514,872,234.88	1,410,220,244.30
无形资产摊销	352,109,903.77	279,526,866.45
长期待摊费用摊销	169,931,231.26	167,301,049.55
报废、处置固定资产、无形资产和其他长期资产 (收益) / 损失	(6,724,858.73)	276,366,964.98
财务净收益	(462,486,041.49)	(280,652,498.25)
投资 (收益) / 亏损	(762,323.82)	18,208,608.90
递延所得税资产 (增加)	(16,405,939.50)	(478,903,221.67)
存货的减少	101,976,794.69	7,432,880.46
经营性应收项目的增加	(2,098,044,036.20)	(527,730,996.56)
经营性应付项目的增加	(1,174,154,670.75)	1,937,053,702.96
经营活动产生的现金流量净额	13,847,728,499.03	17,188,704,639.71

(2) 不涉及现金收支的重大投资和筹资活动：

2022 年度，本公司不涉及现金收支的重大投资和筹资活动主要为因增加使用权资产所确认的租赁负债，金额为人民币 4,867,110,836.42 元(2021 年度：人民币 743,955,240.23 元)。

(3) 现金及现金等价物净变动情况：

	2022 年	2021 年
现金及现金等价物的年末余额	2,091,907,757.12	3,260,263,507.18
减：现金及现金等价物的年初余额	(3,260,263,507.18)	(5,444,859,147.70)
现金及现金等价物净增加额	(1,168,355,750.06)	(2,184,595,640.52)

公共资源交易平台信息专用
AE2C19CEC1F6E1A62A8C88EA14DB9

(4) 本公司持有的现金和现金等价物分析如下：

	2022 年	2021 年
货币资金	2,583,296,896.55	4,636,127,685.66
减：三个月以上银行定期存款	(440,590,000.00)	(1,350,590,000.00)
应收利息	(43,130,843.27)	(13,641,221.38)
使用受限制的货币资金	(7,668,296.16)	(11,632,957.10)
年末现金及现金等价物余额	2,091,907,757.12	3,260,263,507.18

本公司对货币资金结余和使用情况进行监控和管理，对暂无使用计划的货币资金通过存入三个月以上定期存款的方式进行投资。中国移动公司现金及现金等价物中不包含三个月以上定期存款，三个月以上定期存款的变动反映为投资活动的现金流量。

44 其他综合收益的税后净额

	2022 年	2021 年
不能重分类进损益的其他综合收益：		
重新计量设定受益计划变动额	788,848.78	(1,490,000.00)
减：所得税		
小计	788,848.78	(1,490,000.00)
合计	788,848.78	(1,490,000.00)

45 金融工具的风险分析

本公司在正常业务过程中会出现信用风险、流动风险、利率风险、外汇风险和其他价格风险。本公司通过下述财务管理政策和实际操作，对这些风险加以限制。

(1) 信用风险

信用风险，是指金融工具的一方不能履行义务，造成另一方发生财务损失的风险。本公司的信用风险主要来自资产负债表中所列示的货币资金、应收账款、其他应收款以及合同资产。

本公司的绝大部分银行存款存放在中国内地及香港的金融机构，由于大部分交易对方为信誉良好的国有金融机构，因此流动资金的信用风险是有限的。

公共资源交易平台技术专用
AE2C19CEC7F...A62A8DC88EA14DB9

本公司的应收账款主要由客户及其他电信运营商账款结余组成。应收客户账款分布在本公司广大的客户群中。大部分应收个人客户账款允许自账单发出日期起一个月内到期付款。本公司对政企客户授予的业务信用期基于服务合同约定的条款，一般不超过 1 年。其他应收款主要包括应收公用事业押金及租赁押金。本公司管理层已实施信用政策，并且在考虑交易对方的财务状况、本公司以往经验及其他因素的情况下持续监控所承受信用风险的程度。同时，由于本公司的客户基础庞大且互无关联，有关应收款的信用风险集中度有限。因此，管理层认为已经计提的预期信用损失已经反映了应收款不能全额回收的风险。

于 2022 年 12 月 31 日及 2021 年 12 月 31 日，本公司无重大的因债务人抵押而持有的担保物或其他信用增级。

(2) 流动性风险

流动风险是指由于现金流入及流出的时间及数额错配导致当债务到期时没有现金支付的风险。本公司通过持有足够的现金余额以及银行存款 (可随时转换为已知金额的现金)，以应付营运资金、偿付财务公司吸收中国移动公司公司短期存款、支付股息、资本支出等资金需求。

于资产负债表日，本公司各项金融负债以未折现的合同现金流量按到期日列示如下：

	2022 年未折现的合同现金流量					资产负债表账面价值
	1 年内或实时偿还	1 年至 3 年	3 年至 5 年	5 年以上	合计	
应付票据	3,136,885,688.60	-	-	-	3,136,885,688.60	3,136,885,688.60
应付账款	14,595,248,270.40	-	-	-	14,595,248,270.40	14,595,248,270.40
预收账款	4,024,161,161.19	-	-	-	4,024,161,161.19	4,024,161,161.19
其他应付款	518,905,323.55	-	-	-	518,905,323.55	518,905,323.55
租赁负债 (含一年内部分)	1,957,475,549.40	1,224,773,238.20	1,596,204,155.86	1,265,217,049.51	6,043,669,992.97	5,629,061,625.32
合计	24,232,675,993.14	1,224,773,238.20	1,596,204,155.86	1,265,217,049.51	28,318,870,436.71	27,904,262,069.06

	2021 年未折现的合同现金流量					资产负债表账面价值
	1 年内或实时偿还	1 年至 3 年	3 年至 5 年	5 年以上	合计	
应付票据	2,609,680,228.93	-	-	-	2,609,680,228.93	2,609,680,228.93
应付账款	14,711,674,546.57	-	-	-	14,711,674,546.57	14,711,674,546.57
预收账款	6,428,559,468.49	-	-	-	6,428,559,468.49	6,428,559,468.49
其他应付款	558,744,653.49	-	-	-	558,744,653.49	558,744,653.49
租赁负债 (含一年内部分)	1,390,095,685.94	802,931,295.12	266,973,041.86	119,344,162.52	2,579,344,185.44	2,423,156,200.29
合计	25,698,754,583.42	802,931,295.12	266,973,041.86	119,344,162.52	26,888,003,082.92	26,731,815,097.77

于资产负债表日，本公司无重大对外提供的财务担保，亦无重大已签订但尚未开始执行的租赁合同现金流量。

公共资源交易平台投标专用
AE2C19CEC7763E1A218BC0A14DB9

(3) 利率风险

固定利率和浮动利率的带息金融工具分别使本公司面临公允价值利率风险及现金流量利率风险。本公司根据市场环境来决定固定利率与浮动利率工具的比例并通过定期审阅与监察维持适当的固定和浮动利率工具组合。

(a) 本公司于 12 月 31 日持有的带息金融工具如下：

	2022 年	2021 年
固定利率金融工具		
金融资产		
- 货币资金	483,720,843.27	1,364,231,221.38
- 应收资金集中管理款	16,556,707,333.33	17,559,250,036.04
金融负债		
- 一年内到期的非流动负债	1,581,725,815.31	1,306,312,858.53
- 租赁负债	4,047,335,810.01	1,116,843,341.76
合计	22,669,489,801.92	21,346,637,457.71
浮动利率金融工具		
金融资产		
- 货币资金	2,099,576,053.28	3,271,896,464.28
合计	2,099,576,053.28	3,271,896,464.28

于 2022 年 12 月 31 日，在其他变量不变的情况下，假定利率上升 100 个基点将会导致本公司所有者权益增加人民币 15,746,820.40 元(2021 年：人民币 24,539,223.48 元)，净利润增加人民币 15,746,820.40 元 (2021 年：人民币 24,539,223.48 元)。

公共资源交易平台授权专用
AE2C19CEC77646E1A62A8D[illegible]8EA14DB9

46 公允价值

公允价值计量结果所属的层次，由对公允价值计量整体而言具有重要意义的输入值所属的最低层次决定：

第一层次输入值：相同资产或负债在活跃市场上未经调整的报价；

第二层次输入值：除第一层次输入值外，相关资产或负债直接或间接可观察的输入值；

第三层次输入值：相关资产或负债的不可观察输入值。

(1) 持续以公允价值计量的资产——按上述三个层次列示

本公司于 2022 年 12 月 31 日及 2021 年 12 月 31 日无持续的以公允价值计量的资产。

(2) 不以公允价值计量但披露其公允价值的资产和负债

本公司以摊余成本计量的金融资产和金融负债主要包括：应收款项、应付款项等，其账面价值与公允价值无重大差异。

47 资本管理

本公司管理资本的主要目的在于保持合理的资本结构，保障本公司的持续经营能力，从而为股东提供回报。本公司会定期审阅和管理其资本结构，保持资本状况稳健，防范运营风险，同时兼顾在借贷水平较高时取得较佳股东回报，并会根据经济环境的变动对资本结构作出调整。

本公司采用资产负债率来管理资本结构。资产负债率是指总负债和总资产的比率。在年末本公司的资产负债率如下表：

	2022 年	2021 年
总资产	76,674,264,840.93	72,818,501,836.69
总负债	33,385,057,016.17	31,998,166,017.50
资产负债率	44%	44%

本公司不受制于任何外部强制性资本要求。

公共资源交易平台投标专用
AE2C19CEC776A6E1A218BC88EA14DB9

48 承担

资本承担

于 12 月 31 日，本公司的资本承担如下：

项目	2022 年	2021 年
已签订合同	1,600,613,352.79	824,169,086.99

49 资产负债表日后非调整事项

本公司无资产负债表日后非调整事项。

50 关联方关系及其交易

(1) 有关本公司母公司的信息如下：

母公司名称	注册地	业务性质	注册资本	对本公司的持股比例	对本公司的表决权比例
			万元	%	%
中国移动通信有限公司	北京市	通信	5,321,885	100.00	100.00

公共资源交易平台集标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

(2) 本公司与除关键管理人员以外的关联方之间的交易：

(a) 与关联方之间的交易金额如下：

	注	2022 年	2021 年
通信服务收入	注 1	5,021,277.83	4,195,047.24
通信服务支出	注 2	1,340,861,288.67	2,115,741,641.34
房屋场地使用费及物业管理费	注 3	55,960,464.97	185,527,705.49
网络资产租赁及服务费用	注 4	506,901,902.37	550,930,617.14
网内结算收入	注 5	2,054,009,625.56	2,461,999,915.33
网内结算支出	注 5	3,761,649,530.86	4,302,000,167.91
网间结算收入	注 6	40,659,235.79	68,975,161.17
网间结算支出	注 6	59,200,617.37	35,215,633.45
电信业务协作服务费用	注 7	650,651,198.38	555,812,522.40
共享服务费支出	注 8	13,404,953.54	14,081,899.15
股息支付	注 9	6,863,907,654.22	1,549,147,475.46
清算服务费	注 10	172,784,882.62	172,784,882.62
终端及设备采购支出	注 11	1,592,209,296.69	1,272,455,064.81
客服外包费	注 12	1,176,546,067.83	523,269,334.31
网格运营承包费		162,983,251.01	94,706,817.72
业务技术支撑及营销费	注 13	2,865,653,048.94	1,799,114,345.84
利息收入	注 14	5,842,840.71	5,726,025.17
铁塔资产租赁费	注 15	1,130,082,256.21	1,245,397,877.36
铁塔资产服务费	注 16	1,174,432,684.10	1,069,781,263.48

上述与关联方进行的交易是按一般正常商业条款或按相关协议进行的。

公共资源交易平台 仅供查询专用
AE2C19CEC77646E1A62A8D[illegible]A14DB9

注 1：该款项是指已收/应收向浦发银行提供通信服务的收入，按市场价确认。

注 2：该款项是指已付/应付的通信工程规划、设计及施工服务；通信线路及管道的施工服务；通信线路及网络系统维护支撑服务、系统集成、工程监理等服务的款项。相关定价或收费标准参考市场价格或成本加利润的方式经双方协商确定，并在提供相关服务时结算。

注 3：该款项是指就办公室、营业网点的经营租赁而已付/应付中国移动集团公司的房屋场地使用费及物业管理费。租金及物业管理费按照以下其中一项标准确定：(i)独立中介机构评定的价值；(ii)公开渠道获得的适用市场价格或收费标准；或(iii)该方或其子公司向独立第三方收取的价格。

注 4：网络资产使用与租赁是本公司使用关联方的网络资源发生的业务支撑服务及网络资产租赁。业务支持结算款根据中移铁通有限公司在支撑本公司省内固网通信等电信业务时，双方协商一致的固网业务收入的一定比例确认；网络资产租赁根据出租方和本公司(“承租方”)签署的网络资源租用文件及租赁期内网络资源租用确认单，基于市场价格或折旧成本，以不高于向第三方出租同类网络资源的标准结算租赁费用。

注 5：该款项是指本公司已收/应收或已付/应付中国移动通信有限公司的网内结算款项，相关定价或收费标准参考政府指导价、市场价格或成本加利润的方式确定。

注 6：网间结算收支是指与中国移动国际有限公司因国际通信互联互通发生的网间结算款项，参考国际市场相关结算标准由双方协议确定结算价格和方式。

注 7：该款项是指关联方向本公司提供的客户发展服务和电信业务合作产生的费用。根据关联方提供业务代办服务的实际工作量、销售金额、资源投入、资质与牌照使用及发展用户数等指标，参考政府指导价（如有）、市场价或以合理成本加合理利润的方式确定服务收费。

注 8：该款项为本公司就与中国移动集团公司签订的《分享管理服务和分摊管理费协议》，应付/已付中国移动集团公司的综合管理费用，相关定价或收费标准参考政府指导价、市场价格或成本加利润的方式确定。

注 9：该款项为本公司已付中国移动通信有限公司的股息。

注 10：该款项是指本公司已付/应付中国移动有限公司子公司一中移信息技术有限公司的清算服务费，相关定价或收费标准参考市场价格或成本加利润的方式确定。

注 11：该款项为本公司采购商品而应付/已付中国移动通信集团终端有限公司的款项，相关定价或收费标准参考市场价格或成本加利润的方式确定。

公共资源交易电子化技标专用
AE2C19C0A764C1A62A8B0EA14DB9

注 12：该款项是指已付/应付中移在线服务有限公司 10086 客服热线业务支撑费用及实名制查验支撑费用。相关定价或收费标准参考政府指导价并不得高于政府相关文件中规定的上限，同时不低于服务提供方的实际成本。

注 13：该款项是指已付/应付中国移动通信有限公司、亚信科技的技术支撑服务费用。亚信科技：相关定价或收费标准参考政府指导价并以市场价格为准确定。中国移动通信有限公司：根据本公司与中国移动通信有限公司的安排，中国移动通信有限公司代本公司安排广告、展览等和业务技术支撑等服务并统一支付费用；此外其还代本公司向政府支付资源占用费。本公司根据中国移动通信有限公司确定的本公司应承担的前述各项费用支付予中国移动通信有限公司。

注 14：该款项为本公司存放在浦发银行、财务公司的存款产生的利息。适用利率参考中国人民银行公布的基准利率。

注 15：该款项是指因租赁铁塔与铁塔站址场地而应付中国铁塔的租赁费。本公司因租赁铁塔设施（铁塔及场地）、共享铁塔配套设施（如电力设施等)和室内分布系统资源及接收维护等服务应向中国铁塔支付的综合费用开支。根据双方于 2018 年初签署的定价补充协议及之前签署的相关综合服务协议，铁塔相关资产使用及服务的定价主要基于相关资产的折旧成本、场租、维护费用与其他开支等因素，以一定的成本加成率和共享折扣率计算确定。

注 16：该款项是指因使用铁塔机房配套、维护电力、室分产品及其他资产而应付中国铁塔的铁塔服务费。

(b) 与关联方之间的交易于 12 月 31 日的余额如下：

	2022 年	2021 年
货币资金	822,377,537.38	2,034,755,266.02
应收账款	1,493,391,836.22	851,970,960.14
预付账款	369,352.28	17,161,950.31
应收资金集中管理款	16,556,707,333.33	17,559,250,036.04
使用权资产	4,466,813,734.95	1,216,004,185.40
应付账款	5,910,700,562.46	5,269,652,506.34
应付票据	1,300,110,501.27	1,014,422,786.72
预收款项	30,274,107.73	34,980,275.34
其他应付款	4,414,450.00	246,500.00
租赁负债	4,523,521,146.96	1,259,346,015.80

公共资源交易平台授权专用

(c) (2)(a) 和 (b) 中涉及交易的关联方与本公司的关系

企业名称	与本公司关系
中国移动通信集团有限公司	本公司的最终控股公司
中国移动通信有限公司	本公司的母公司
中国移动（香港）集团有限	与本公司同受最终母公司控制
中国移动香港 BVI 有限公司	与本公司同受最终母公司控制
中移集团基础设施控股有限公司	与本公司同受最终母公司控制
中移集团基础设施有限公司 1	与本公司同受最终母公司控制
中移集团基础设施有限公司 2	与本公司同受最终母公司控制
数据空间有限公司	与本公司同受最终母公司控制
中移集团基础设施有限公司 3	与本公司同受最终母公司控制
中国移动有限公司	与本公司同受最终母公司控制
中国移动投资有限公司	与本公司同受最终母公司控制
中移信息技术有限公司	与本公司同受最终母公司控制
ASPIRE HOLDINGS LIMITED	与本公司同受最终母公司控制
卓望（BVI）有限公司	与本公司同受最终母公司控制
卓望（香港）集团有限公司	与本公司同受最终母公司控制
卓望信息技术（北京）有限公司	与本公司同受最终母公司控制
卓望信息技术（西安）有限公司	与本公司同受最终母公司控制
卓望数码技术（深圳）有限公司	与本公司同受最终母公司控制
中国移动香港有限公司	与本公司同受最终母公司控制
Advanced Roaming & Clearing House	与本公司同受最终母公司控制
中国移动国际控股有限公司	与本公司同受最终母公司控制
中国移动国际有限公司	与本公司同受最终母公司控制
中国移动国际（英国）有限公司	与本公司同受最终母公司控制
中国移动国际（美国）有限公司	与本公司同受最终母公司控制
中国移动美国科技有限公司	与本公司同受最终母公司控制
中国移动国际株式会社	与本公司同受最终母公司控制
中国移动国际（德国）有限公司	与本公司同受最终母公司控制
中国移动国际（澳洲）有限公司	与本公司同受最终母公司控制
中国移动国际（加拿大）有限公司	与本公司同受最终母公司控制
中国移动国际（韩国）有限公司	与本公司同受最终母公司控制
中国移动国际（巴西）有限公司	与本公司同受最终母公司控制

公共资源交易平台会员专用
AE2C19C[illegible]6E1A62[illegible]A14DB9

企业名称	与本公司关系
中国移动国际（巴西）信息科技有限公司	与本公司同受最终母公司控制
中国移动国际（法国）有限公司	与本公司同受最终母公司控制
中国移动国际（南非）有限公司	与本公司同受最终母公司控制
中国移动国际（巴拿马）有限公司	与本公司同受最终母公司控制
中国移动国际（意大利）有限公司	与本公司同受最终母公司控制
中国移动国际（瑞士）有限公司	与本公司同受最终母公司控制
中国移动国际（墨西哥）信息科技有限公司	与本公司同受最终母公司控制
中国移动国际（新加坡）有限公司	与本公司同受最终母公司控制
中国移动国际（马来西亚）有限公司	与本公司同受最终母公司控制
中国移动国际（阿联酋）有限公司	与本公司同受最终母公司控制
中国移动国际（俄罗斯）有限公司	与本公司同受最终母公司控制
中国移动国际技术（越南）有限公司	与本公司同受最终母公司控制
中国移动国际（泰国）有限公司	与本公司同受最终母公司控制
中国移动国际（肯尼亚）信息科技有限公司	与本公司同受最终母公司控制
中国移动（柬埔寨）信息科技有限公司	与本公司同受最终母公司控制
中国移动国际（印度尼西亚）有限公司	与本公司同受最终母公司控制
中国移动国际基础设施控股有限公司	与本公司同受最终母公司控制
中国移动国际基础设施（BVI）（SG1）有限公司	与本公司同受最终母公司控制
中国移动国际基础设施（SG1）有限公司	与本公司同受最终母公司控制
中国移动国际基础设施（BVI）（US1）有限公司	与本公司同受最终母公司控制
中国移动国际基础设施（US1）有限公司	与本公司同受最终母公司控制
中国移动国际基础设施（BVI）（UK1）有限公司	与本公司同受最终母公司控制
中国移动国际基础设施（BVI）（GER1）有限公司	与本公司同受最终母公司控制
中国移动国际基础设施（BVI）（US2）有限公司	与本公司同受最终母公司控制
GB21（香港）有限公司	与本公司同受最终母公司控制
中国移动通信集团广东有限公司	与本公司同受最终母公司控制
中国移动粤港澳大湾区（广东）创新研究院有限公司	与本公司同受最终母公司控制
中国移动通信集团浙江有限公司	与本公司同受最终母公司控制
浙江移动信息系统集成有限公司	与本公司同受最终母公司控制
中国移动（浙江）创新研究院有限公司	与本公司同受最终母公司控制
中国移动通信集团江苏有限公司	与本公司同受最终母公司控制
江苏移动信息系统集成有限公司	与本公司同受最终母公司控制

公共资源交易中心专用
AE2C19C[illegible]1A82[illegible]A14DB9

企业名称	与本公司关系
中国移动紫金（江苏）创新研究院有限公司	与本公司同受最终母公司控制
中国移动通信集团福建有限公司	与本公司同受最终母公司控制
福建福诺移动通信技术有限公司	与本公司同受最终母公司控制
中国移动通信集团海南有限公司	与本公司同受最终母公司控制
中国移动通信集团北京有限公司	与本公司同受最终母公司控制
北京融昱信息技术有限公司	与本公司同受最终母公司控制
中国移动通信集团上海有限公司	与本公司同受最终母公司控制
上海中移信息技术有限公司	与本公司同受最终母公司控制
中国移动通信集团天津有限公司	与本公司同受最终母公司控制
中国移动通信集团河北有限公司	与本公司同受最终母公司控制
中国移动通信集团辽宁有限公司	与本公司同受最终母公司控制
辽宁中移通信技术工程有限公司	与本公司同受最终母公司控制
中国移动通信集团山东有限公司	与本公司同受最终母公司控制
山东中移通信技术有限公司	与本公司同受最终母公司控制
中国移动通信集团广西有限公司	与本公司同受最终母公司控制
中国移动通信集团安徽有限公司	与本公司同受最终母公司控制
中国移动通信集团江西有限公司	与本公司同受最终母公司控制
中移（江西）虚拟现实科技有限公司	与本公司同受最终母公司控制
中国移动通信集团重庆有限公司	与本公司同受最终母公司控制
中国移动通信集团四川有限公司	与本公司同受最终母公司控制
中国移动通信集团湖北有限公司	与本公司同受最终母公司控制
湖北中移通信技术工程有限公司	与本公司同受最终母公司控制
中国移动通信集团湖南有限公司	与本公司同受最终母公司控制
湖南中移通信技术工程有限公司	与本公司同受最终母公司控制
中国移动通信集团陕西有限公司	与本公司同受最终母公司控制
陕西中移通信技术工程有限公司	与本公司同受最终母公司控制
中国移动通信集团山西有限公司	与本公司同受最终母公司控制
中国移动通信集团内蒙古有限公司	与本公司同受最终母公司控制
中国移动通信集团吉林有限公司	与本公司同受最终母公司控制
中国移动通信集团黑龙江有限公司	与本公司同受最终母公司控制
黑龙江中移通信技术工程有限公司	与本公司同受最终母公司控制
中国移动通信集团贵州有限公司	与本公司同受最终母公司控制

公共资源交易平台专用
AE2C19C[illegible]1A62[illegible]A14DB9

企业名称	与本公司关系
中移园区建设发展有限公司	与本公司同受最终母公司控制
贵州移动信息科技有限公司	与本公司同受最终母公司控制
中国移动通信集团云南有限公司	与本公司同受最终母公司控制
中国移动通信集团西藏有限公司	与本公司同受最终母公司控制
中国移动通信集团甘肃有限公司	与本公司同受最终母公司控制
中国移动通信集团青海有限公司	与本公司同受最终母公司控制
中国移动通信集团宁夏有限公司	与本公司同受最终母公司控制
中国移动通信集团新疆有限公司	与本公司同受最终母公司控制
中国移动通信集团设计院有限公司	与本公司同受最终母公司控制
北京煜金桥通信建设监理咨询有限责任公司	与本公司同受最终母公司控制
中移数智科技有限公司	与本公司同受最终母公司控制
中国移动通信集团终端有限公司	与本公司同受最终母公司控制
中国移动通信集团财务有限公司	与本公司同受最终母公司控制
中移物联网有限公司	与本公司同受最终母公司控制
芯昇科技有限公司	与本公司同受最终母公司控制
中移（苏州）软件技术有限公司	与本公司同受最终母公司控制
中移（杭州）信息技术有限公司	与本公司同受最终母公司控制
中移系统集成有限公司	与本公司同受最终母公司控制
咪咕文化科技有限公司	与本公司同受最终母公司控制
咪咕音乐有限公司	与本公司同受最终母公司控制
咪咕视讯科技有限公司	与本公司同受最终母公司控制
上海咪咕新媒体有限公司	与本公司同受最终母公司控制
咪咕数字传媒有限公司	与本公司同受最终母公司控制
咪咕互动娱乐有限公司	与本公司同受最终母公司控制
咪咕动漫有限公司	与本公司同受最终母公司控制
中移在线服务公司	与本公司同受最终母公司控制
中移互联网有限公司	与本公司同受最终母公司控制
中移投资控股有限责任公司	与本公司同受最终母公司控制
中移铁通有限公司	与本公司同受最终母公司控制
山东铁通工程建设有限责任公司	与本公司同受最终母公司控制
沈阳华铁通信工程监理有限公司	与本公司同受最终母公司控制
中移铁通云科技有限公司	与本公司同受最终母公司控制
北京北方星辰信息技术有限公司	与本公司同受最终母公司控制

公共资源交易平台 仅供专用
AE2C19C[illegible]45E1A62[illegible]A14DB9

企业名称	与本公司关系
中移（上海）商业保理有限公司	与本公司同受最终母公司控制
中移金科控股有限公司	与本公司同受最终母公司控制
中移建设有限公司	与本公司同受最终母公司控制
四川中移通信技术工程有限公司	与本公司同受最终母公司控制
中国铁通集团（香港）有限	与本公司同受最终母公司控制
中国铁通香港电信有限公司	与本公司同受最终母公司控制
中移雄安信息通信科技有限公司	与本公司同受最终母公司控制
中移（成都）信息通信科技有限公司	与本公司同受最终母公司控制
中移（上海）信息通信科技有限公司	与本公司同受最终母公司控制
中移动金融科技有限公司	与本公司同受最终母公司控制
海达保险经纪有限公司	与本公司同受最终母公司控制
中移动信息技术有限公司	与本公司同受最终母公司控制
中移电子商务有限公司	与本公司同受最终母公司控制
中移信息系统集成有限公司	与本公司同受最终母公司控制
天威通信有限公司	与本公司同受最终母公司控制
FU HAO PROPERTIES LIMITED	与本公司同受最终母公司控制
Extra Step Investments Limited	与本公司同受最终母公司控制
福建迅捷通信技术服务有限公司	与本公司同受最终母公司控制
河南省飞达通信开发有限公司	与本公司同受最终母公司控制
郑州梨园村实业有限公司	与本公司同受最终母公司控制
海南省信通通信服务有限公司	与本公司同受最终母公司控制
三沙华海通信服务有限公司	与本公司同受最终母公司控制
北京通信服务有限公司	与本公司同受最终母公司控制
北京移联信达通信技术有限公司	与本公司同受最终母公司控制
上海通信服务有限公司	与本公司同受最终母公司控制
天津通信服务有限公司	与本公司同受最终母公司控制
河北通信服务有限公司	与本公司同受最终母公司控制
辽宁通信服务有限公司	与本公司同受最终母公司控制
山东通信服务有限公司	与本公司同受最终母公司控制
广西通信服务有限公司	与本公司同受最终母公司控制
安徽通信服务有限公司	与本公司同受最终母公司控制
江西中移通信服务有限公司	与本公司同受最终母公司控制
江西省邮电技工学校	与本公司同受最终母公司控制

公共资源交易平台专用
AE2C19C[illegible]16E1A62[illegible]A14DB9

企业名称	与本公司关系
重庆通信服务有限公司	与本公司同受最终母公司控制
四川通信服务有限公司	与本公司同受最终母公司控制
湖北通信服务有限公司	与本公司同受最终母公司控制
湖南通信服务有限公司	与本公司同受最终母公司控制
陕西通信实业有限公司	与本公司同受最终母公司控制
山西通信服务有限公司	与本公司同受最终母公司控制
内蒙古通信服务有限公司	与本公司同受最终母公司控制
吉林中移通信服务有限公司	与本公司同受最终母公司控制
吉林省邮电防腐厂	与本公司同受最终母公司控制
黑龙江通信服务有限公司	与本公司同受最终母公司控制
贵州中移通信服务有限公司	与本公司同受最终母公司控制
云南通信服务有限公司	与本公司同受最终母公司控制
西藏通信服务有限公司	与本公司同受最终母公司控制
甘肃通信服务有限公司	与本公司同受最终母公司控制
青海通信服务有限公司	与本公司同受最终母公司控制
宁夏通信服务有限公司	与本公司同受最终母公司控制
新疆通信服务有限公司	与本公司同受最终母公司控制
中京通信服务有限公司	与本公司同受最终母公司控制
辛姆巴科有限公司	与本公司同受最终母公司控制
中国铁通集团有限公司	与本公司同受最终母公司控制
中铁通信中心	与本公司同受最终母公司控制
中移资本控股有限责任公司	与本公司同受最终母公司控制
中移创业投资有限责任公司	与本公司同受最终母公司控制
北京中移和创股权投资合伙企业（有限合伙）	与本公司同受最终母公司控制
中移智行网络科技有限公司	与本公司同受最终母公司控制
中国移动慈善基金会	与本公司同受最终母公司控制
中国移动香港（BVI）有限公司	与本公司同受最终母公司控制
Teleinfo Limited	与本公司同受最终母公司控制
海南省通信服务有限公司	与本公司同受最终母公司控制
吉林通信服务有限公司	与本公司同受最终母公司控制
中国移动辛姆巴科有限公司	与本公司同受最终母公司控制
试金石信用服务有限公司	母公司的合营企业
安徽科大讯飞信息科技股份有限公司	母公司的联营企业

公共资源交易平台专用
AE2619C...A61A62...A14DB9

企业名称	与本公司关系
中国铁塔股份有限公司	母公司的联营企业
福建和颐健康科技发展有限公司	受同一控制方控制的其他子公司的合营企业
中移创新产业基金（深圳）合伙企业（有限合伙）	受同一控制方控制的其他子公司的合营企业
AsiaInfo Technologies Limited	受同一控制方控制的其他子公司的联营企业
上海浦东发展银行股份有限公司	受同一控制方控制的其他子公司的联营企业
香港润迅通信联合有限公司	受同一控制方控制的其他子公司的联营企业
广东中建通信服务有限公司	受同一控制方控制的其他子公司的联营企业
北京质码科技有限公司	受同一控制方控制的其他子公司的联营企业
正数网络技术有限公司	受同一控制方控制的其他子公司的联营企业
浙江省新型互联网交换中心有限责任公司	受同一控制方控制的其他子公司的联营企业
True Corporation Public Company Limited	受同一控制方控制的其他子公司的联营企业
北京青牛技术股份有限公司	受同一控制方控制的其他子公司的联营企业
深圳市润迅通信联合有限公司	受同一控制方控制的其他子公司的联营企业
深圳市前海新型互联网交换中心有限公司	受同一控制方控制的其他子公司的联营企业
哈尔滨能创科技有限责任公司	受同一控制方控制的其他子公司的联营企业
宁夏中卫市新型互联网交换中心有限责任公司	受同一控制方控制的其他子公司的联营企业
南京创芯慧联技术有限公司	受同一控制方控制的其他子公司的联营企业
北京海誉动想科技股份有限公司	受同一控制方控制的其他子公司的联营企业
寰宇信任（北京）技术有限公司	受同一控制方控制的其他子公司的联营企业
北京海天瑞声科技股份有限公司	受同一控制方控制的其他子公司的联营企业
信通数智量子科技有限公司	受同一控制方控制的其他子公司的联营企业
招商局仁和人寿保险股份有限公司	最终控股公司的联营企业
云南通信股份有限公司	最终控股公司的其他子公司的联营企业
新疆尊茂银都酒店有限责任公司	最终控股公司的其他子公司的联营企业
北京京都信苑饭店有限公司	最终控股公司的其他子公司的联营企业
北京市瑞迪通无线通信技术服务有限公司	最终控股公司的其他子公司的联营企业
宁夏虹桥大酒店有限责任公司	最终控股公司的其他子公司的联营企业
芒果超媒股份有限公司	最终控股公司的其他子公司的联营企业
数字广东网络建设有限公司	最终控股公司的其他子公司的联营企业

公共资源交易平台 仅供专用
AE2C19CEC...A14DB9

企业名称	与本公司关系
凤凰卫视投资(控股)有限公司	最终控股公司的其他子公司的联营企业
中国民航信息网络股份有限公司	最终控股公司的其他子公司的联营企业
联仁健康医疗大数据科技股份有限公司	最终控股公司的其他子公司的联营企业
北京华宇软件股份有限公司	最终控股公司的其他子公司的联营企业
中移股权基金管理有限公司	最终控股公司的其他子公司的联营企业
中移股权基金(河北雄安)合伙企业(有限合伙)	最终控股公司的其他子公司的联营企业
分海（香港）有限公司	最终控股公司的其他子公司的联营企业
分海有限公司	最终控股公司的其他子公司的联营企业
中国通信服务股份有限公司	公司内董监高在外任职企业
世纪畅链有限责任公司	公司内董监高在外任职企业
上海分互链信息技术有限公司	公司内董监高在外任职企业
嘉华国际集团有限公司	公司内董监高在外任职企业
天安中国投资有限公司	公司内董监高在外任职企业
开达集团有限公司	公司内董监高在外任职企业
北京第四范式智能技术股份有限公司	公司内董监高在外任职企业
中国建筑股份有限公司	公司内董监高在外任职企业

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9



统一社会信用代码

91110000599649382G

营业执照

（副 本）(3-1)

名　　称　毕马威华振会计师事务所（特殊普通合伙）

类　　型　台港澳投资特殊普通合伙企业

执行事务合伙人　邹俊

经营范围　审查企业会计报表，出具审计报告；验证企业资本，出具验资报告；办理企业合并、分立、清算事宜中的审计业务，出具有关报告；基本建设年度财务决算审计；代理记账；会计咨询、税务咨询、管理咨询、会计培训；法律、法规规定的其他业务。（市场主体依法自主选择经营项目，开展经营活动；依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动；不得从事国家和本市产业政策禁止和限制类项目的经营活动。）

出　资　额　12164万元

成立日期　2012年7月10日

主要经营场所　北京市东城区东长安街1号东方广场东2座办公楼8层

登记机关　北京市市场监督管理局

2022年 12 月 30 日

国家企业信用信息公示系统网址：http://www.gsxt.gov.cn

市场主体应当于每年1月1日至6月30日通过国家企业信用信息公示系统报送公示年度报告。

国家市场监督管理总局监制

本文件仅用于出具业务报告目的使用，不得作任何其他用途



会计师事务所

执业证书

名　　称：毕马威华振会计师事务所（特殊普通合伙）

首席合伙人：邹俊

主任会计师：

办公场所：北京市东长安街1号东方广场东2座办公楼8层

组织形式：特殊的普通合伙企业

会计师事务所编号：11000241

注册资本(出资额)：人民币壹亿零壹拾伍万元整

批准设立文号：财会函〔2012〕31号

批准设立日期：二〇一二年七月五日

证书序号：000421

说　明

1、《会计师事务所执业证书》是证明会计师事务所经财政部门依法审批、准予从事注册会计师法定业务的凭证。

2、《会计师事务所执业证书》[illegible]项发生变更，应当向财政部门申请换发。

3、《会计师事务所执业证书》不得伪造、变造、出租、出借、转[illegible]

4、会计师事务所终止，应当向财政部门交回《会计师事务所执业证书》。

发证机关：

二〇一五年　四月　二日

中华人民共和国财政部制

公共资源交易平台投标专用
AE2019CEC77[illegible]A618BC88EA14DB9
此复印件仅供出具业务报告用的使用，其他用途无效





姓　　名
Full name　　[illegible]
性　　别
Sex　　[illegible]
出 生 日 期
Date of birth　　[illegible]
工 作 单 位
Working unit　　[illegible]
身份证号码
Identity card No.　　[illegible]



公共资源交易平台投标专用
AE2C19CEC77646E[illegible]2A8BC88EA14DB9

注册会计师工作单位变更事项登记
Registration of the Change of Working Unit by a CPA

同意调出
Agree the holder to be transferred from

事务所
CPAs

毕马威华振会计师事务所

转出协会盖章
Stamp of the transfer-out Institute of CPAs

年 2012
月 8
日 20

同意调入
Agree the holder to be transferred to

事务所
CPAs

毕马威华振会计师事务所(特殊普通合伙)

转入协会盖章
Stamp of the transfer-in Institute of CPAs

年 2012
月 8
日 20

注册会计师工作单位变更事项登记
Registration of the Change of Working Unit by a CPA

同意调出
Agree the holder to be transferred from

事务所
CPAs

转出协会盖章
Stamp of the transfer-out Institute of CPAs

年
月
日

同意调入
Agree the holder to be transferred to

事务所
CPAs

转入协会盖章
Stamp of the transfer-in Institute of CPAs

年
月
日

11

公共资源交易平台投标专用
AE2C19CEC7764E1452A8F288EA14DB9

公共资源交易中心投标专用
AE2C19CEC778[illegible]88EA14DB9





姓　　名
Full name　高林
性　　别
Sex　男
出生日期
Date of birth　1988-10-18
工作单位
Working unit　毕马威华振会计师事务所（特殊普通合伙）
身份证号码
Identity Card No.　230623198810180055





公共资源交易平台投标专用
AE2C19CEC77646E1[illegible]8C88EA14DB9

公共资源交易平台投标专用
AE2C19CEC77646E1A6218C88EA14DB9

8.2 投标人企业财务会计制度

第一章　总则

第一条　为规范公司财务会计行为，依据《会计法》、《企业财务通则》和《企业会计准则》等有关法律、法规，结合本公司的实际情况，制定本制度。

第二条　公司会计工作的基本任务是贯彻执行国家财政政策和会计法规，强化财务管理，加强财务监督，规范各项财务收支的计划控制、核算、分析和考核工作，如实反映公司财务状况和经营成果，依法纳税，为公司领导当好参谋，为公司决策，为企业创造最大利润。

第三条　公司会计工作由公司财务部负责。财务应当根据《会计法》的规定，确保公司会计工作和会计资料的真实性和完整性；负责公司财务计划的制定和监督检查，协助公司制定经营方针和资本运作政策；负责公司会计机构的设置，对财会人员的配备、考核和奖惩提出建议，并确保会计机构、会计人员依法履行职责；负责协调金融、财政、税务、审计、证券监管等方面的关系。

第四条　公司设立财务部，负责财务会计方面的日常工作，财务部经理负责公司财务收支计划的执行，主管公司的会计核算和资金管理工作，主持制定公司的财务规章制度，规范各级财务管理实施细则，统一公司会计核算办法，配合财务协调外部关系。

第五条　公司会计机构和会计人员应当依照会计法律法规的规定，按照真实、完整的要求，进行会计核算，实行会计监督，并向公司汇报会计工作情况，报送财务会计报告和其他必要资料。

第六条　公司会计年度采用公历年度，会计核算以人民币为记账本位币，会计记账采用借贷记账法。

第七条　公司审核原始凭证、填制会计凭证、登记会计账簿、编报财务会计报告和管理会计档案，应当遵循有关法律法规和本制度的要求。

第二章　会计管理体制

第八条　公司财务会计根据岗位职责分工负责本公司的财务会计工作，并对会计工作和会计资料的真实性和完整性负责，财务部负责具体的日常会计工作。

第九条　公私财务负责人为财务会计，依法行如下会计管理职责：

（一）　依法设立会计机构、配备会计人员，并支持他们的工作，保障会计人员依法履行职责；

（二）　正确执行相关法律法规和规章制度，纠正违反财务会计制度的行为；

（三）　最终审批公司所有财务支出事项；

（四）　对会计工作情况及会计资料的真实性、完整性负责，签署对外公布的财务会计报告；

（五）　法律法规规定或上级主管部门授予的其他职责。

第十条　会计机构应当按照有关法律法规的规定、上级主管部门及公司主要负责人的要求，强化会计岗位责任制度、内部控制制度和会计稽核制度。

第十一条　公司领导、部门经理其他员工应当按照本制度的规定，在各自的权限内真实、完整的审核和提供各种经济业务的原始资料。公司有关人员在对所管业务的财务收支进行具体的预算管理和目标控制时，对有关的原始资料负有记录、保管和及时进行传递的责任。

第三章　主要会计政策

第十二条　本公司执行的会计及财务制度为：《会计法》、《企业会计制度》、《公司经营企业会计制度》等。

第十三条　以每年元月一日至十二月三十一日为一个会计年度。

第十四条　记帐原则和方法：以权责发生制为原则，实行借贷记账法。

第十五条　企业的会计核算以人民币为记账本位币。

第十六条　公司的固定资产按直线法计提折旧。

第十七条　按照有关规定计提坏账准备，存货跌价准备和其他资产减值准备。

第四章　会计科目的设置

第十八条　公司执行财政部颁发的《企业会计制度》，《企业会计准则》和《公司经营企业会计制度》，并根据具体经营特点选用总账会计科目，其明细科目根据编制报表要求，按便于理解，方便管理和符合公司经济活动分析的需要合理设置。

第二十八条　财务部在具体帐务处理中必须正确使用确定的会计科目，在实际工作中可根据实际情况适当增设相关会计科目。

第五章　会计账簿的设置

第十九条　财务部按《会计法》的规定，设置会计账簿，包括总账、明细帐、日记张和其他辅助性账簿。

第二十条　根据电算化的要求，当期所有记账凭证数据和明细账数据都储存于计算机。

第二十一条　明细账根据会计核算系统，结帐后数据自动生成资产、负债、权益、损益四大类明细账。账本格式按照会计科目的设置、管理查账的需要，合理编排为借贷余三栏式、成本费用类多栏式、多借一贷式、多贷一借式和多借多贷式。

第二十二条　日记账分为银行日记账和先进日记账，不得跨年度使用，账簿不得用银行对账单或其他方式代替。开设若干个银行存款账户时，应按开设的账户分别登记银行日记账，日记账由出纳根据银行收（付）款、现金收（付）款凭证登记，按凭证发生日期、凭证号依次登记，做到日清月结，登记时不得出现银行存款或现金的红字。

第二十三条　各种租借设备、物资、有价证券、应收应付票据、项目核算资料等应设置辅助账。各种帐簿必须有统一固定的格式，要做到内容真实完整、数字准确、摘要清楚、登记及时，不漏记、错记或重记。如果发生错误或者隔页、跳行的，应按规定的办法更正，并由会计人员和会计机构负责人在更正处盖章。

第二十四条　财务部应按规定定期对会计账簿纪录金额与库存金额、货币资金、有价证券、往来单位或个人等进行核实，做到帐证、帐账、帐表、帐实相符，对帐工作每年至少一次，如遇人员调动或发生非常事件，也应及时对帐。

第二十五条　会计账簿安银行存款日记账、现金日记账、总账、明细帐、辅助账分别整理立卷，归档保管。

第二十六条　本公司使用财务会计软件进行会计核算，软件输出的会计帐簿应当符合国家统一会计制度的要求，并及时装订。除会计软件输出的正式帐簿外，不得设立其它正式帐簿。通过会计软件输出的正式帐簿，应当按照封面、扉页、科目发生额及余额表、总账和明细账的顺序进行打印和装订，各科目的总账和明细账按科目编号的顺序宁打印和装订。

公司证券事务专用

第六章　　固定资产的核算

第二十七条　使用年限在一年（不含一年）以上，单位价值在2000元（不含2000元）以上，并在使用过程中保持原有物质形态的资产，包括房屋及建筑物、电子设备、运输设备、机器设备、工具、器具。当一项固定资产的某组成部分在使用效能上与流动资产相对独立，并且具有不同使用年限时，应将该组成部分单独确认为固定资产。

第二十八条　财务部门要定期对固定资产、低值易耗品进行全面盘点、清查，每年年终前为定期盘点清查的时间。

第二十九条　所有固定资产和低值易耗品都必须按国家有关规定进行折旧或摊销。

第三十条　对固定资产盘盈、盘亏，由财务部、行政事务部调查核实，弄清情况，提出意见，逐笔报领导审批，财务部门根据规定作帐务处理。

第七章　　货币资金的核算

第三十一条　公司的货币资产包括现金、银行存款和其它货币资金。

第三十二条　财务部门必须定期或不定期对货币资金进行盘点、对帐，并确保账款相符。

第三十三条　货币资金管理必须遵守《货币资金管理制度》的有关规定。

第八章　　经营成本的核算

第三十四条　在公司业务经营中发生的与经营有关的各项支出等按规定计入成本。

第三十五条　营业及管理费用主要包括：职工工资、职工福利费、广告及业务宣传费、业务招待费、差旅费、水电费、租赁费、员工培训经费、办公费、会议费、其它费用等。

第三十六条　费用控制及管理严格按有关制度执行。

第九章　　经营收入的核算

第三十七条　经营收入是指业务经营过程中取得营业性收入。

第三十八条　代理性业务只将公司代理费计入公司营业收入。

第三十九条　一般贸易类业务可按交易额计算公司营业收入。

第十章　　纳税、利润及其分配

第四十条　本公司利润总额按下列公式计算：

利润总额=营业利润+投资收益+营业外收支净额

净利润=利润总额-应纳所得税

营业利润=主营业务收入-主营业务成本+其它业务利润-营业费用-管理费用-财务费用

国债投资收益根据规定不缴企业所得税。

第四十一条　所得税后利润根据公司章程的规定，按如下顺序分配：

（一）　弥补上一年度的亏损；

（二）　提取法定公积金10%；

（三）　提取任意公积金；

（四）　支付股东股利；

公司法定公积金累计为公司注册资本的50%以上的，可以不再提取。提取法定公积金后，是否提取任意公积金由股东大会决定。公司不在弥补亏损和提取法定公积金、或公益金之前向股东分配利润。

第四十二条 本公司须依法申报和交纳营税、城市维护建设税、教育费附加、房产税、土地使用税、车船使用税、印花税、企业所得税及其他应纳税种。

第十一章 会计报表的种类与编制

第四十三条 会计人员应当根据会计账簿的记录编制会计报表。本公司应分年，半年、季度和月度填制下列报表。

第四十四条 企业向外提供的会计报表包括：资产负债表；利润表；现金流量表；资产减值准备明细表；利润分配表；股东权益增减变动表；分部报表；其他有关附表。内部管理报表主要由银行存款收支月报表、成本月报表、债权债务明细表等，企业应根据管理的实际需要设计编制内部管理报表，并根据企业发展需要增加或减少报表种类，调整报表内容、报表格式。内部管理财务报表的设计、编制、报送须经财务副总批准，其它任何部门和人员无权直接要求财务部门提供财务报表、财务数据。

第十二章 会计工作交接

第四十五条 会计人员调动或离职，必须将本人所经管的会计工作全部移交给接替人员。未办清交接手续的，不得调动或离职。

第四十六条 接替人员应当认真接管移交工作，并继续办理移交的未了事项。离职会计人员办理移交手续前，必须及时做好以下工作：

（一） 已受理的经济业务尚未填制会计凭证的，应当填制完毕；

（二） 为登记账目应当登记完毕，并在最后一笔余额后加盖经办人员印章；

（三） 整理应该移交的各项资料，对未了事项写出书面材料；

（四） 编制已较轻册，列明应当移交的会计凭证、会计账簿、会计报表、印章、现金、有价证券、支票簿、发票、文件、财务软件及密码、数据瓷盘及有关资料等。

第四十七条 会计人员办理移交时，必须有监交人负责监交。一般会计人员交接，由财务部经理或副经理负责监交；财务部经理或副经理交接，由公司分管财务工作的财务副总（或其授权代理人）负责监交。

第四十八条 移交人员在办理移交时，要按移交清册逐项移交；接替人员要逐项核对查收。一脚人员从事会计电算化工作的，要对有关电子数据在实际操作状态下进行交接。

第四十九条 财务部副经理以及以上级别的财务人员移交时，还必须将全部财务会计工作、重大财务收支和会计人员的情况等向接替人员详细介绍。对需要移交的遗留问题，应当写出书面材料。

第五十条 交接完毕后，交接双方和监交人员要在移交注册上签名或者盖章，并应在移交清册页数上注明：单位名称，交接日期，交接双方和监交人员的职务、姓名，移交清册页数以及需要说明的问题和意见等。移交清册一般应当填制一式三份，交接双方各执一份，存档一份。

第五十一条 接替人员应当继续使用移交的会计账簿，不得自行另立新帐，以保持会计记录的连续性。

第十三章 附则

第五十二条 本制度由中国移动通信集团河南有限公司财务部负责解释和修订。

九、投标人出具 2020 年以来在经营活动中没有重大违法记录的书面声明（加盖单位公章）



投标人出具 2020 年以来在经营活动中没有重大违法记录的书面声明

致：南阳市政务服务和大数据管理局（采购人名称）

中国移动通信集团河南有限公司（投标人名称）郑重声明，我方参加本项目招标活动，自 2020 年以来在经营活动中没有重大违法记录，符合《中华人民共和国政府采购法》规定的供应商资格条件。我方对此声明负全部法律责任。

特此声明。



投 标 人（公章）：中国移动通信集团河南有限公司

时间：2023 年 12 月 7 日

公共资源交易平台投标专用
AE2C19CEC77646E1A[illegible]88EA14DB9

十、投标人出具信用记录查询结果网页截图

10.1 失信被执行人查询截图



2023/12/6 16:06 全国法院失信被执行人名单信息公布与查询

(http://zxgk.court.gov.cn/)

失信被执行人将在政府采购、招标投标、行政审批、政府扶持、融资信贷、市场准入、资质认定等方面受到信用惩戒！

失信被执行人(自然人)公布

姓名/名称	证件号码
钟来平	5129211973****3853
雍先全	5129011961****2911
张雪飞	1302811988****005X
丁朝伦	5102321963****6314
何智南	5130011977****0846

失信被执行人(法人或其他组织)公布

姓名/名称	证件号码
星河互联集团有限公司	69167076-6
北京佳士壮服饰贸易有限公司	06727935-X
北京溢思得瑞智能科技研究院有限公司	MA005UR8-3
北京东方易美装饰有限公司	75333755-6

查询条件

被执行人姓名/名称:

中国移动通信集团河南有限公司

身份证号码/组织机构代码:

91410000719172532Q

省份:

----------全部----------

验证码:

Masv

Masv

验证码正确!

查询

查询结果

zxgk.court.gov.cn/shixin/ 1/2

公共资源交易平台投标专用
A6E19CEC17646E1A62A8BC88EA14DB9

在全国范围内没有找到 91410000719172532Q 中国移动通信集团河南有限公司相关的结果.

全国法院失信被执行人名单信息公布与查询平台首页

声明

为推进社会信用体系建设，对失信被执行人进行信用惩戒，促使其自动履行生效法律文书确定的义务，根据《中华人民共和国民事诉讼法》相关规定，最高人民法院制定了《关于公布失信被执行人名单信息的若干规定》，自今日起向社会开通“全国法院失信被执行人名单信息公布与查询”平台，社会各界通过该平台查询全国法院（不包括军事法院）失信被执行人名单信息。现就有关事项作出如下声明：

一、被执行人未履行生效法律文书确定的义务，并具有《最高人民法院关于公布失信被执行人名单信息的若干规定》第一条规定的情形之一的，执行法院将根据申请执行人的申请或依职权决定将该被执行人纳入失信被执行人名单，并通过该网站予以公布。

二、各级人民法院将向政府相关部门、金融监管机构、金融机构、承担行政职能的事业单位及行业协会等通报失信被执行人名单信息，供相关单位依照法律、法规和有关规定，在政府采购、招标投标、行政审批、政府扶持、融资信贷、市场准入、资质认定等方面，对失信被执行人予以信用惩戒；将向征信机构通报失信被执行人名单信息，并由征信机构在其征信系统中记录。

国家工作人员、人大代表、政协委员等被纳入失信被执行人名单的，失信情况将通报其所在单位和相关部门；国家机关、事业单位、国有企业等被纳入失信被执行人名单的，失信情况将通报其上级单位、主管部门或者履行出资人职责的机构。

三、纳入失信被执行人名单的被执行人，执行法院将根据《最高人民法院关于限制被执行人高消费及有关消费的若干规定》第一条的规定，对被执行人采取限制消费措施。

被执行人为自然人的，被采取限制消费措施后，不得有以下高消费及非生活和工作必需的消费行为：（一）乘坐交通工具时，选择飞机、列车软卧、轮船二等以上舱位；（二）在星级以上宾馆、酒店、夜总会、高尔夫球场等场所进行高消费；（三）购买不动产或者新建、扩建、高档装修房屋；（四）租赁高档写字楼、宾馆、公寓等场所办公；（五）购买非经营必需车辆；（六）旅游、度假；（七）子女就读高收费私立学校；（八）支付高额保费购买保险理财产品；（九）乘坐G字头动车组列车全部座位、其他动车组列车一等以上座位等其他非生活和工作必需的消费行为。被执行人为单位的，被采取限制消费措施后，被执行人及其法定代表人、主要负责人、影响债务履行的直接责任人员、实际控制人不得实施前述行为。因私消费以个人财产实施前述行为的，可以向执行法院提出申请。

四、被纳入失信被执行人名单的公民、法人或其他组织认为有《最高人民法院关于失信被执行人名单信息的若干规定》第十一条规定情形之一的，可以向执行法院申请纠正。

五、本网站提供的信息仅供查询人参考。如有争议，以执行法院有关法律文书为准。因使用本网站信息而造成不良后果的，人民法院不承担任何责任。

六、查询人必须依法使用查询信息，不得用于非法目的和不正当用途。非法使用本网站信息给他人造成损害的，由使用人自行承担相应责任。

七、本网站信息查询免费，严禁任何单位和个人利用本网站信息牟取非法利益。

八、本网站属于政府网站，未经许可，任何商业性网站不得建立与本网站及其内容的链接，不得建立本网站的镜像（包括全部和局部镜像），不得拷贝、复制或传播本网站信息。

九、如对该查询内容有异议，请与执行法院联系。

最高人民法院

2013年10月8日

地址：北京市东城区东交民巷27号 邮编：100745

总机：010-67550114

中华人民共和国最高人民法院 版权所有

京ICP备05023036号

公共资源交易平台专供专用
AE2C19CEC776...F1A62A8BC88EA14DB9

10.2 重大税收违法失信主体查询截图



公共资源交易平台投标专用
AE2019CEC77646E1A62A8BC88EA14DB9

10.3 政府采购严重违法失信行为记录查询截图



公共资源交易平台投标专用
AE2019CEC77646E1A62A8BC88EA14DB9

10.4 中国政府采购网政府采购严重违法失信行为记录查询截图

公共资源交易平台投标专用

10.5 不存在《中华人民共和国政府采购法实施条例》第十九条规定的行政处罚记录的承诺函

致：南阳市政务服务和大数据管理局（采购人名称）

中国移动通信集团河南有限公司（投标人名称）郑重声明，我方不存在《中华人民共和国政府采购法实施条例》第十九条规定的行政处罚记录，符合《中华人民共和国政府采购法》规定的供应商资格条件。我方对此声明负全部法律责任。

特此声明。

投 标 人（公章）：中国移动通信集团河南有限公司

时间：2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C19CEC77646E1[illegible]8EA14DB9

10.6 投标人信用报告



信用中国
WWW.CREDITCHINA.GOV.CN

扫一扫
核验码

法人和非法人组织公共信用信息报告

版本号V2.0

机构名称： 中国移动通信集团河南有限公司

统一社会信用代码： 91410000719172532Q

报告编号： 202312201930215252E970

报告生成日期	2023年12月20日
报告出具单位	国家公共信用信息中心

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20231220193021525 2E970
生成时间：2023年12月20日 19:30:21

扫一扫
核验码

公共信用信息概览

中国移动通信集团河南有限公司

存续　守信激励对象

基础信息

统一社会信用代码	91410000719172522Q	法定代表人/负责人/执行事务合伙人	楼向平
企业类型	有限责任公司(外商投资企业法人独资)	成立日期	1999-08-06
住所	郑州市经三路48号		

信用信息概要

行政管理	53条	诚实守信	4条
严重失信	0条	经营异常	0条
信用承诺	73条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2023年12月20日	报告出具单位	国家公共信用信息中心

报告编号：20231220193021525 2E970
生成时间：2023年12月20日 19:30:21

扫一扫
核验码

报告说明

1.本报告所展示的数据和资料为公共信用信息，“信用中国”网站承诺在数据汇总、加工、整合的过程中保持客观中立，不主动编辑或修改信息内容。

2.受限于现有技术水平等原因，对此报告信息的展示，并不视为“信用中国”对其内容的真实性、准确性、完整性、时效性作出任何形式的确认或担保，请在依据本报告信息作出判断或决策前，自行进一步核实此类信息的完整或准确性，并自行承担使用后果。

3.如认为本报告所展示信息存在错误、遗漏、重复公示、不应公示、超期公示或与认定机关信息不一致等情况，请以数据源单位的信息为准，并可按照网站“信用信息异议申诉指南”提出异议申诉；如需对相关行政处罚信息进行信用修复，可按照网站“行政处罚信息信用修复流程指引”提出信用修复申请；如需对相关严重失信主体名单进行信用修复，请咨询名单认定单位。

4.本报告已添加“信用中国”水印、生成唯一的报告编号和报告核验码。如需对内容的真实性进行核验，可通过扫一扫报告首页“核验码”，查看本报告生成时的内容与纸质版报告内容是否一致。

5.本报告展示行政管理、诚实守信、严重失信、经营异常、信用承诺、信用评价、司法判决以及其他类等信息，因篇幅有限，单类信息仅按更新程度展示最近日期的100条。如有特殊需求，请与我们联系。

报告编号：20231220193021525 2E970
生成时间：2023年12月20日 19:30:21

扫一扫
核验码

正文

存续 守信激励对象

中国移动通信集团河南有限公司

一、登记注册基础信息

企业名称：	中国移动通信集团河南有限公司
统一社会信用代码：	9141000071917 2532Q
法定代表人/负责人/执行事务合伙人：	楼向平
企业类型：	有限责任公司(外商投资企业法人独资)
成立日期：	1999-08-06
住所：	郑州市经三路48号

二、行政管理信息 (共 53 条)

行政许可

行政许可决定文书号：	郑港建消审字〔2023〕第0019号	第 1 条
行政许可决定文书名称：	特殊建设工程消防设计审查意见书	
许可证书名称：	——	
许可类别：	核准	
许可编号：	——	
许可决定日期：	2023-08-10	
有效期自：	2023-08-10	
有效期至：	2099-12-31	
许可内容：	中国移动（河南）数据中心项目	
许可机关：	郑州航空港经济综合实验区建设局(郑州市生态环境局郑州航空港经济综合实验区分局)	
许可机关统一社会信用代码：	11410100680759247K	
数据来源单位：	郑州航空港经济综合实验区建设局(郑州市生态环境局郑州航空港经济综合实验区分局)	

数据来源单位统一社会信用代码： 11410100680759247K

行政许可

第 2 条

行政许可决定文书号： 许准字〔2023〕04350号

行政许可决定文书名称： 准予行政许可决定

许可证书名称： 特种设备使用登记证

许可类别： 普通

许可编号： 梯11豫A14606(23)

许可决定日期： 2023-07-27

有效期自： 2023-07-27

有效期至： 2038-07-27

许可内容： 特种设备使用登记证梯11豫A14606(23)

许可机关： 郑州航空港经济综合实验区市场监督管理局

许可机关统一社会信用代码： 11410100080809 60X2

数据来源单位： 郑州航空港经济综合实验区市场监督管理局

数据来源单位统一社会信用代码： 11410100080809 60X2

行政许可

第 3 条

行政许可决定文书号： 郑开环安审〔2023〕8号

行政许可决定文书名称： 关于《中国移动通信集团河南有限公司中国移动（河南郑州）数据中心备用发电机项目》的批复

许可证书名称： ——

许可类别： 认可

许可编号： ——

许可决定日期： 2023-03-14

有效期自： 2023-03-15

有效期至：	2099-12-31
许可内容：	我局批准本项目，原则同意你公司按照《报告表》所列项目性质、规模、地点、采用的生产工艺和环境保护对策措施进行项目建设。
许可机关：	郑州高新技术产业开发区管委会环保安监局
许可机关统一社会信用代码：	114101000052545
数据来源单位：	郑州高新技术产业开发区管委会环保安监局
数据来源单位统一社会信用代码：	11410100005254528Y

行政许可

行政许可决定文书号：	许准字〔2022〕03971号	第 4 条
行政许可决定文书名称：	准予行政许可决定书	
许可证书名称：	特种设备使用登记证	
许可类别：	普通	
许可编号：	梯12豫A05459(22)	
许可决定日期：	2022-07-18	
有效期自：	2022-07-18	
有效期至：	2037-07-18	
许可内容：	特种设备使用登记证梯12豫A05459(22)	
许可机关：	郑州航空港经济综合实验区市场监督管理局	
许可机关统一社会信用代码：	1141010008080960X2	
数据来源单位：	郑州航空港经济综合实验区市场监督监督管理局	
数据来源单位统一社会信用代码：	1141010008080960X2	

行政许可

行政许可决定文书号：	许准字〔2022〕03950号	第 5 条

行政许可决定文书名称：	特种设备使用登记证
许可证书名称：	特种设备使用登记证
许可类别：	普通
许可编号：	梯11豫A15932(22)
许可决定日期：	2022-07-15
有效期自：	2022-07-15
有效期至：	2037-07-15
许可内容：	特种设备使用登记证梯11豫A15932(22)
许可机关：	郑州航空港经济综合实验区市场监督管理局
许可机关统一社会信用代码：	1141010008080960X2
数据来源单位：	郑州航空港经济综合实验区市场监督监督管理局
数据来源单位统一社会信用代码：	1141010008080960X2

行政许可

第 6 条

行政许可决定文书号：	牟水许准字〔2021〕第84号
行政许可决定文书名称：	准予行政许可决定书
许可证书名称：	——
许可类别：	普通
许可编号：	——
许可决定日期：	2021-09-28
有效期自：	2021-09-28
有效期至：	2099-12-31
许可内容：	同意通过审批
许可机关：	中牟县水利局
许可机关统一社会信用代码：	1141012200529508XU
数据来源单位：	中牟县水利局

数据来源单位统一社会信用代码： 1141012200529508XU

行政许可

第 7 条

行政许可决定文书号： JY3[illegible]1010504497 62

行政许可决定文书名称： 食品卫生经营许可证

许可证书名称： — —

许可类别： 登记

许可编号： — —

许可决定日期： 2021-08-31

有效期自： 2021-08-31

有效期至： 2099-12-31

许可内容： 食品经营

许可机关： 郑州市金水区市场监督管理局

许可机关统一社会信用代码： 11410105MB1666058T

数据来源单位： 郑州市金水区市场监督管理局

数据来源单位统一社会信用代码： 11410105MB1666058T

行政许可

第 8 条

行政许可决定文书号： 牟建消审字〔2020〕第0030号

行政许可决定文书名称： 特殊建设工程消防设计审查意见书

许可证书名称： — —

许可类别： 核准

许可编号： — —

许可决定日期： 2020-07-31

有效期自： 2020-07-31

有效期至：	2099-07-31
许可内容：	允许施工
许可机关：	中牟县住房和城乡建设局
许可机关统一社会信用代码：	11410122MB1650494R
数据来源单位：	中牟县住房和城乡建设局
数据来源单位统一社会信用代码：	11410122MB165

行政许可

行政许可决定文书号：	410122202007310301	第 9 条
行政许可决定文书名称：	建筑工程施工许可证	
许可证书名称：	— —	
许可类别：	核准	
许可编号：	— —	
许可决定日期：	2020-07-31	
有效期自：	2020-07-31	
有效期至：	2099-12-31	
许可内容：	根据《中华人民共和国建筑法》第八条规定，经审查，本建筑工程符合施工条件，准予施工。	
许可机关：	中牟县住房和城乡建设局	
许可机关统一社会信用代码：	11410122MB1650494R	
数据来源单位：	中牟县住房和城乡建设局	
数据来源单位统一社会信用代码：	11410122MB1650494R	

行政许可

行政许可决定书文号：	郑环审201832号	第 10 条
许可有效期：	— —	

许可决定日期： 2018-02-11

许可截止日期： 2099-12-31

许可内容： 郑州市环境保护局关于中国移动河南郑州数据中心项目配套110kV输变电工程环境影响报告表报批版的批复

许可机关： 郑州市环境保护局

审核类型： 普通

行政许可

行政许可决定书文号： 许环辐审〔2017〕1号 第 11 条

许可有效期： — —

许可决定日期： 2017-01-03

许可截止日期： — —

许可内容： 建设项目环境影响评价

许可机关： 许昌市环保局

审核类型： 普通

行政许可

行政许可决定书文号： 牟政港土201643号 第 12 条

许可有效期： — —

许可决定日期： 2016-12-05

许可截止日期： 2066-09-29

许可内容： 国有土地使用权出让面积：109423.4平方米

许可机关： 中牟县人民政府航空港实验区

审核类型： 普通

行政许可

行政许可决定书文号： 郑震许字〔2016〕第261号 第 13 条

许可有效期： ——

许可决定日期： 2016-06-06

许可截止日期： 2099-12-31

许可内容： 权限内建设工程抗震设防要求确定

许可机关： 郑州市地震局

审核类型： 普通

行政许可

行政许可决定书文号： 郑震许字〔2016〕第261号 第 14 条

许可有效期： ——

许可决定日期： 2016-06-06

许可截止日期： 2099-12-31

许可内容： 权限内建设工程抗震设防要求确定

许可机关： 郑州市地震局

审核类型： 普通

行政许可

行政许可决定书文号： 郑水行许[2016]9号 第 15 条

许可有效期： ——

许可决定日期： 2016-04-06

许可截止日期： 2099-12-31

许可内容： 中国移动通信集团河南有限公司用水指标核准许可

许可机关： 郑州市水务局

审核类型： 普通

行政许可

行政许可决定书文号：	洛环[2016]2号	第 16 条
许可有效期：	— —	
许可决定日期：	2016-03-08	
许可截止日期：	2099-12-31	
许可内容：	根据《中国移动通信集团河南有限公司洛阳数据中心工程建设项目环境影响报告表》（以下简称《报告表》）的分析结论、专家技术函审意见，我局原则批准该项目《报告表》，同意该项目按相关规定报批建设。n一、中国移动通信集团河南有限公司洛阳数据中心工程主要建设机房楼、研发中心和生产调度用房等，本项目为互联网服务项目，符合洛阳经济技术产业集聚区发展规划，符合国家产业政策。n二、建设单位在建设过程中要全面落实《报告表》中提出的各项污染防治措施，认真执行环境保护“三同时”制度。重点要求如下：n 1、施工期间必须采取有效措施，减少开挖基础、装卸、运输等过程产生的二次扬尘污染。n2、生活污水经化粪池处理后水质均符合《污水综合排放标准》（GB8978-1996）表4中三级标准，排入市政污水管网进入洛阳市新区污水处理厂进一步处理。n3、报废的电脑和服务器属于危险废物，应按危废管理要求存放在暂存间，定期委托有资质的单位处理，危险废物在转移前，要按照相关规定到环保部门办理危废转移手续。n 4、生活垃圾经垃圾箱收集后交由当地环卫部门统一处置。n 5、建设单位应向社会公众主动公开已经批准的《报告表》、并接受相关方面的垂询。n三、该项目主要污染物总量控制指标以建设项目主要污染物总量控制指标为：COD 12.2378t/a，NH3-N 1.2719t/a 。 n 四、中国移动通信集团河南有限公司洛阳数据中心工程项目竣工后，按规定程序向洛龙环境保护分局申请竣工环境保护验收，经验收合格，方可正式投入运行。n 五、洛龙环境保护分局负责对本项目日常环境监督管理工作，监督项目环保“三同时”的落实。	
许可机关：	洛阳市环境保护局洛龙环境保护分局	
审核类型：	普通	

行政许可

行政许可决定书文号：	豫环审〔2016〕136号	第 17 条
许可有效期：	— —	
许可决定日期：	2016-02-25	
许可截止日期：	— —	
许可内容：	一、《报告表》内容符合国家有关法律法规要求和建设项目环境管理规定，评价结论可信。我厅批准该《报告表》，原则同意你公司按照《报告表》所列项目的性质、规模、地点、采用的生产工艺和环境保护对策进行项目建设。nn 二、你公司应向社会公众主动公开业经批准的《报告表》，并接受相关方的咨询。nn 三、你公司应全面落实《报告表》提出的各项环境保护措施，确保各项环境保护设施与主体工程同时设计、同时施	

工、同时投入使用，确保各项污染物达标排放。nn（一）向设计单位提供《报告表》和本批复文件，确保项目设计按照环境保护设计规范要求，落实防治环境污染和生态破坏的措施以及环保设施投资概算。nn（二）依据《报告表》和本批复文件，对项目建设过程中产生的废水、废气、固体废物、噪声、振动等污染，以及因施工对自然、生态环境造成的破坏，采取相应的防治措施。nn（三）项目外排污染物应满足以下要求：nn 1. 废气。施工期，应加强施工监管，采取低扬尘施工工艺、施工材料堆存点设置围挡、运输车辆加盖篷布等措施，严格控制施工扬尘，废气排放应满足《大气污染物综合排放标准》（GB16297-1996）中相关标准，同时应满足《河南省蓝天工程行动计划》、《郑州市控制扬尘污染工作方案的通知》的要求。运营期，食堂油烟采用油烟净化设施处理后排放，应满足《饮食业油烟排放标准（试行）》（GB18483-2001）要求。nn 2. 噪声。施工期，应加强施工噪声监管，通过选用低噪声设备、合理安排高噪声设备作业时间、施工场地远离敏感点、设置施工围挡等措施，减轻施工噪声对周围居民的影响，噪声排放应满足《建筑施工场界环境噪声排放标准》（GB12523-2011）要求。运营期噪声应满足《工业企业厂界环境噪声排放标准》（GB12348-2008）3类标准要求。nn 3. 废水。施工期，施工废水经沉淀后回用，生活污水经化粪池处理后排入市政污水管网。运营期，生活污水经化粪池处理后，与中央空调循环冷却排污水一起排入城市污水处理厂进一步处理。废水排放应满足《污水综合排放标准》（GB8978-1996）表4三级标准和城市污水处理厂进水水质的要求。 nn 4. 固废。各种固废应妥善处置或综合利用。一般固体废物临时贮存按《一般工业固体废物贮存、处置场污染控制标准》（GB18599-2001）进行控制。施工期，建筑垃圾和渣土应及时清运至环卫部门指定

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2016〕70号　　第 18 条

许可有效期： — —

许可决定日期： 2016-01-22

许可截止日期： — —

许可内容： 一、《报告表》内容符合国家有关法律法规要求和建设项目环境管理规定，评价结论可信。我厅批准该《报告表》，原则同意你公司按照《报告表》所列项目的性质、规模、地点、采用的生产工艺和环境保护对策进行项目建设。nn 二、你公司应向社会公众主动公开业经批准的《报告表》，并接受相关方的咨询。nn 三、你公司应全面落实《报告表》提出的各项环境保护措施，确保各项环境保护设施与主体工程同时设计、同时施工、同时投入使用，确保各项污染物达标排放。nn（一）向设计单位提供《报告表》和本批复文件，确保项目设计按照环境保护设计规范要求，落实防治环境污染和生态破坏的措施以及环保设施投资概算。nn（二）依据《报告表》和本批复文件，对项目建设过程中产生的废水、废气、固体废物、噪声、振动等污染，以及因施工对自然、生态环境造成的破坏，采取相应的防治措施。nn（三）项目外排污染物应满足以下要求：nn 1. 废气。施工期，应加强施工监管，采取低扬尘施工工艺、施工材料堆存点设置围挡、运输车辆加盖篷布等措施，严格控制施工扬尘。运营期，食堂油烟采用油烟净化设施处理后排放，应满足《饮食业油烟排放标准（试行）》（GB18483-2001）要求。nn 2. 噪声。施工期，应加强施工噪声监管，通过选用低噪声设备、合理安排高噪声设备作业时间、施工场地远离敏感点、设置施工围挡等措施，减轻施工噪声对周围居民的影响，噪声排放应满足《建筑施工场界环境噪声排放标准》（GB12523-2011）要求。运营期噪声应满足《社会生活环境噪声排放标准》(GB22337-2008)2类标准。nn 3. 废水。施工期，施工废水经沉淀后回用，生活污水经化粪池处理后排入市政管网。运营期，生活污水经化粪池处理后与中央空调循环冷却排污水一起经市政管网排入城市污水处

理厂进一步处理。废水排放应满足《污水综合排放标准》（GB8978-1996）表4三级标准和城市污水处理厂进水水质的要求。 nn 4. 固废。各种固废应妥善处置或综合利用。一般固体废物临时贮存按《一般工业固体废物贮存、处置场污染控制标准》（GB18599-2001）进行控制。施工期，建筑垃圾和渣土应及时清运至环卫部门指定的处置场所。运营期，生活垃圾由市政部门定期清运；化粪池污泥采用密闭罐车清运。nn 四、如果今后国家或我省颁布新标准，届时你公司应按新标准执行。nn 五、本批复

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2015〕470号　　第 19 条

许可有效期： — —

许可决定日期： 2015-11-27

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求nn 本期项目共报批10270个基站（新建基站5654个，扩建基站4616个），批准建设10270个基站（见附件）。本期建设基站天线类型均为定向型；GSM网基站设备标称功率为8瓦和20瓦，TD-SCDMA网基站设备标称功率为12瓦和20瓦，TD-LTE网基站设备标称功率均为20瓦；项目总投资96185万元，其中环保投资4150万元。nn 以上项目在落实《报告表》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告表所列项目的内容、地点及采取的环境保护措施进行建设。nn 二、你单位应向社会公众主动公开已经批准的《报告表》，并接受相关方的咨询。nn 三、项目建设和运营中应重点做好的工作nn（一）本批项目基站应严格按报告表规划的地址建设，并将项目的电磁环境关注区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保环境和公众安全。nn（二）落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。nn（三）采取降噪措施，保证机房等设施产生的噪声达到标准要求。nn（四）基站运行过程中产生的废旧蓄电池应按照国家有关规定进行处理，不得随意丢弃，避免造成环境污染。nn（五）落实环境风险防范措施，制定环境风险应急预案，加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。nn 四、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测，发现问题及时采取措施加以解决。nn 五、新建项目建设应严格执行配套建设的环境保护设施与主体工程同时设计、同时施工、同时投产的环境保护“三同时”制度。项目必须按照规定程序申请竣工环境保护验收，验收合格后方可正式投入运行。工程中分期建设的项目，可分期申请验收。nn 六、我厅委托河南省辐射环境安全技术中心和当地省辖市、省直管县环保局负责项目施工期和运营期的环境保护监督检查工作。nn 七、本批复有效期五年。本项目自批复之日起五年后开工建设的，应报我厅重新审核。本批复生效后，建设项目的地点、规模、技术参数等发生变化时，应重新编制环境影响评价文件报我厅审核。

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2015〕121号　　第 20 条

许可有效期： — —

许可决定日期： 2015-04-16

许可截止日期： — —

许可内容： 一、项目建设内容和要求nn 本期项目共报批15089个基站，均已经建成投入使用（本次环评抽测467个典型基站，占全部基站总数的30.61%），建设地点位于河南省16个省辖市及10个直管县（基站见附件）。nn 二、《报告书》的结论和现状监测结果表明，项目产生的电磁辐射功率密度和噪声均能满足国家相关标准的要求，生态影响得到了有效恢复，我厅同意本批项目继续运行。nn 三、你单位应进一步完善各项环保管理制度，加强电磁污染防治设施的管理，保障设施正常运行。废旧蓄电池必须按照有关规定交有资质的单位回收处理。nn 四、定期对基站主要污染因子进行监测，并及时向环保部门报告监测情况。nn 五、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。nn 六、我厅委托河南省辐射环境安全技术中心和各省辖市、直管县环保局负责该项目日常监督检查工作。

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2015〕122号　　第 21 条

许可有效期： — —

许可决定日期： 2015-04-16

许可截止日期： — —

许可内容： 一、本期验收工程包括中国移动通信集团河南有限公司GSM网、TD-SCDMA网基站建设项目中已经建成投入使用的4517个基站（抽测1387个典型基站，占全部基站总数的30.70%）。建设地点位于河南省17个省辖市及7个直管县（基站名单见附表）。nn 二、我厅同意验收组意见，该项目环保审批手续齐全，环境保护设施均按照环评文件和省环保厅批复要求进行了落实，基站产生的电磁辐射功率密度和噪声均能满足国家相关标准的要求，生态影响得到有效恢复，同意通过验收。nn 三、你单位应进一步完善各项环保管理制度，加强电磁污染防治设施的管理，保障设施正常运行。废旧蓄电池必须按照有关规定交有资质的单位回收处理。nn 四、定期对基站主要污染因子进行监测，并及时向环保部门报告监测情况。nn 五、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。nn 六、我厅委托河南省辐射环境安全技术中心和各省辖市、直管县环保局负责该项目日常监督检查工作。

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2015〕120号　　第 22 条

许可有效期： — —

许可决定日期： 2015-04-16

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求nn本期项目共报批9947个基站，其中新建基站9362个，已建基站585个（属专项行动清查基站,见附件2）。批准建设9945个基站（见附件3），2个基站不予审批（见附件1）。本期建设基站天线类型均为定向型；GSM网基站和TD-SCDMA网基站设备标称功率均为20瓦，TD-LTE网基站设备标称功率为12/15/20瓦；项目总投资146195万元，其中环保投资4463.5万元。nn 以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。nn 二、你单位应向社会公众主动公开已经批准的《报告书》，并接受相关方的咨询。nn 三、项目建设和运营中应重点做好的工作nn（一）基站建设应科学规划，合理选址，按照报告书所列的相关要求设置电磁环境关注区域和警示标志,并将本批项目的电磁环境关注区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保环境和公众安全。nn（二）落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。nn（三）采取降噪措施，保证机房等设施产生的噪声达到标准要求。nn（四）基站运行过程中产生的废旧蓄电池应按照国家有关规定进行处理，不得随意丢弃，避免造成环境污染。nn（五）落实环境风险防范措施，制定环境风险应急预案，加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。nn 四、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测，发现问题及时采取措施加以解决。nn 五、新建项目建设应严格执行配套建设的环境保护设施与主体工程同时设计、同时施工、同时投产的环境保护“三同时”制度。项目必须按照规定程序申请竣工环境保护验收，验收合格后方可正式投入运行。工程中分期建设的项目，可分期申请验收。nn 六、我厅委托河南省辐射环境安全技术中心和当地省辖市、省直管县环保局负责项目施工期和运营期的环境保护监督检查工作。nn 七、本批复有效期五年。本项目自批复之日起五年后开工建设的，应报我厅重新审核。本批复生效后，建设项目的地点、规模、技术参数等发生变化时，应

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2014〕602号　　第 23 条

许可有效期： — —

许可决定日期： 2014-12-31

许可截止日期： — —

许可内容： 一、工程建设内容。本期验收工程包括中国移动通信集团河南有限公司2013-2014年GSM网、TD-SCDMA/LTE网基站建设项目中已经建成投入使用的17103个基站（其中GSM网2725个、TD-SCDMA网6047个、TD-LTE网8331个），建设地点位于河南省18个省辖市及10个直管县。nn 二、中国电子工程设计院编制的《中国移动通信集团河南有限公司2013-2014年GSM网、TD-SCDMA/LTE网基站建设项目竣工环境保护验收调查报告（总报告各省辖市、直管县分册）》表明：nn 该项目环保审批手续齐全，环境保护设施均按照环评和省环保厅批复要求进行了落实，基站产生的电磁辐射功率密度和噪声均能满足国家相关标准的要求，生态影响得到有效恢复，我厅同意各省辖市、直管县环保局验收组意见，17101个基站（见附件）通过验收，2个基站暂缓通过验收。nn 三、你单位应进一步完善各项环保管理制度，加强电磁污染防治设施的管理，保障设施正常运行。废旧蓄电池必须交有资质的单位回收处理。定期对基站主要污染因子进行监测，并及时向有关部门报告监测情况。加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。nn 四、你单位应按照规定办理《电磁辐射环境验收合格证》。各省辖市、直管县环保局监督检查。nn 五、我厅委托河南省辐射环境安全技术中心和各省辖市、直管县环保局负责日常监督检查工作。

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2014〕604号　　第 24 条

许可有效期： — —

许可决定日期： 2014-12-31

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求nn 本期项目共报批20525个基站，批准建设20445个基站（见附件），80个暂缓审批。本期建设基站天线类型均为定向型；GSM基站设备发射功率为20瓦，TD-SCDMA基站设备发射功率为10/12/16/20瓦，TD-LTE基站设备发射功率为2/10/12/16/20/25瓦；本批基站中单站为7324个，共站建设13201个；总投资348821.5万元，其中环保投资9899.7万元。nn 以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。nn 二、你单位应向社会公众主动公开已经批准的《报告书》，并接受相关方的咨询。nn 三、项目建设和运营中应重点做好的工作nn（一）基站建设应科学规划，合理选址，按照报告书所列的相关要求设置电磁环境关注区域和警示标志，限制公众在电磁环境关注区域内的活动。并将本批项目的电磁环境关注区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保环境和公众安全。nn（二）落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。nn（三）采取降噪措施，保证机房等设施产生的噪声达到标准要求。nn（四）落实环境风险防范措施，制定环境风险应急预案，加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。nn 四、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测，发现问题及时采取措施加以解决。nn 五、项目建设应严格执行配套建设的环境保护设施与主体工程同时设计、同时施工、同时投产的环境保护“三同时”制度。项目试运行时，向环保部门报告；试运行三个月内，必须按照规定程序申请竣工环境保护验收，验收合格后方可正式投入运行。工程中分期建设的项目，可分期申请验收。nn 六、我厅委托河南省辐射环境安全技术中心和当地省辖市、省直管县环保局负责项目施工期和运营期的环境保护监督检查工作。nn 七、本批复有效期五年。本项目自批复之日起五年后开工建设的，应报我厅重新审核。本批复生效后，建设项目的地点、规模、技术参数等发生变化时，应重新编制环境影响评价文件

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2014〕26 第 25 条

许可有效期： — —

许可决定日期： 2014-07-14

许可截止日期： — —

许可内容： 一、本期验收工程包括中国移动通信集团河南有限公司2013年GSM网、TD-SCDMA网基站建设项目中已经建成投入使用的基站6530个（基站分布情况见附件），建设地点均位于河南省境内。nn 二、《调查报告》表明：该项目环保审批手续齐全，环境保护设施均按照环评和省环保厅批复要求进行了落实，基站的各项环境污染因子能够达到相关标准的要求，生态影响得到了有效恢复。nn 三、我厅同意当地省辖市、省直管县环保局及验收组意见，同意通过验收。nn 四、你单位应进一步完善各项环保管理制度，加强电磁污染防治设施的管理，保障设施正常运行。废旧蓄电池应按照国家相关规定交有资质的单位回收处理。nn 五、项目正式运行后要做好电磁、声环境的日常监测工作。nn 六、要加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。nn 七、我厅委托河南省辐射环境安全技术中心和当地省辖市、省直管县环保局负责日常监督检查工作。

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2014〕260号 第 26 条

许可有效期： — —

许可决定日期： 2014-07-14

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求nn 本期项目共报批20762个基站，批准建设20747个基站，15个基站不符合审批要求不予审批（见附件）。本期建设基站天线类型为定向型和全向型；采用落地铁塔、落地美化塔、落地独管塔、落地三管塔、落地增高架、楼顶抱杆、楼顶增高架、楼顶美化天线、楼顶角钢塔、室内分布等10种架设方式，其中落地铁塔6893个、落地美化塔1363个、落地独管塔909个、落地三管塔214个、落地增高架1072个、楼顶抱杆2897个、楼顶增高架5272个、楼顶美化天线1727个、楼顶角钢塔358个、室内分布42个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为9瓦、20瓦和40瓦、TD-LTE网为20瓦和40瓦；GSM900网天线上行发射频段为890~909兆赫兹，下行发射频段为935～954兆赫兹，GSM1800网天线

上行发射频段为1710~1725兆赫兹，下行发射频段为1805~1820兆赫兹，TD-SCDMA网频段为2010~2025兆赫兹，TD-LTE网频段为1880~1900兆赫兹（F频段）、2500~2690兆赫兹（D频段）；本批基站中单站建设6365个，共站建设14382个。nn 本期项目总投资411183.8万元，其中环保投资11644.5万元，占总投资的2.83%。nn 以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。nn 二、你单位应向社会公众主动公开已经批准的《报告书》，并接受相关方的咨询。nn 三、项目建设和运营中应重点做好以下工作nn（一）基站建设应科学规划，合理选址，按照报告书所列的相关要求设置辐射防护区域和警示标志，限制公众在辐射防护区域内的活动。并将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保环境和公众安全。nn（二）落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。nn（三）基站运行过程中产生的废旧蓄电池应按照国家有关规定进行处理，不得随意丢弃，避免造成环境污染。nn（四）采取降噪措施，保证机房等设施产生的噪声达到标准要求。nn

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫无办〔2013〕38号　　第 27 条

许可有效期： — —

许可决定日期： 2013-12-26

许可截止日期： — —

许可内容： <p style="TEXT-ALIGN: center; TEXT-INDENT: 2em">关于中国移动河南有限公司办理2013年基站建设事宜的批复</p><p> </p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">中国移动通信集团河南有限公司：</p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">你公司《中国移动河南公司关于办理2013年基站设站手续的请示》（豫移文〔2013〕1590号）收悉，按照国家设台审批程序相关规定要求，现批复如下：</p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">申请建设的约12000个TD-LTE基站数量不准确、资料</p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">不齐全，应提供：</p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">1、TD-LTE网络建设（无线部分）设计书（包括技术原理、详细的网络建设方案等）。</p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">2、基站分布、站址、经纬度、基站设备（型号及型号核准证）、基站类型（宏站、拉远等）、天馈。</p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">3、申请建设基站数量应确切。</p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">4、共建共享基站必须注明（已存在的网络技术体制、设备数量等）。</p><p> </p><p style="TEXT-ALIGN: left; TEXT-INDENT: 2em">

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕234号 第 28 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站49个（其中GSM网工程43个，TD-SCDMA网工程6个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶增高架3种架设方式，其中落地铁塔46个，独管塔2个，楼顶增高架1个，并建设相应配套设施；基站设备标称发射功率GSM网为20/30瓦、TD-SCDMA网为20瓦；GSM900天线上行发射频段分别为890～909兆赫兹，下行发射频段分别为935～954兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站4个，GSM900与联通共站1个，其余均为独站；总投资1445.6万元，其中环保投资92.3万元，占总投资的6.38%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离27.4米、垂直防护距离4.0米；TD-SCDMA单站最大水平防护距离16.3米、垂直防护距离3.5米；GSM900 和TD-SCDMA 共站最大水平防护距离29.9米、垂直防护距离8.0米；GSM900 和联通共站最大水平防护距离29.2米、垂直防护距离4.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。n三、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测，发现问题及时采取措施加以解决。n四、项目建设应严格执行配套建设的环境保护设施

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕231号 第 29 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站89个（其中GSM网工程35个，TD-SCDMA网工程54个），其天线类型全部为定向型；采用落地铁塔，楼顶抱杆，楼顶增高架，美化天线4种架设方式，其中落地铁塔30个，楼顶抱杆19个，楼顶增高架30个，美化天线10个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦，TD-SCDMA网为12瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站9个，其余均为独站；总投资2382万元，环保投资110.5万元，占总投资的4.64%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区域，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离5.5米，TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离3.0米；GSM900与TD-SCDMA共站情况下最大水平防护距离23.5米、垂直防护距离6.0米,在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。 n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。n三、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测，发现问题及时采取措施加以解决。n四、项目建设应严格执行配套建设的环境

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕236号　　第 30 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站54个（其中GSM网工程44个，TD-SCDMA网工程10个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、楼顶增高架、美化天线5种架设方式，其中落地铁塔32个，独管塔5个，楼顶抱杆7个，楼顶增高架8个，美化天线2个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站8个，GSM900与联通共站2个，GSM900与电信基站共站1个，其余均为独站；总投资3742.1万元，其中环保投资229万元，占总投资的

6.12%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离4.0米；GSM900 和TD-SCDMA 共站最大水平防护距离21.6米、垂直防护距离4.5米；GSM900 和联通、电信共站最大水平防护距离26.9米、垂直防护距离5.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。n三、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕232号　　第 31 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站46个（其中GSM网工程34个，TD-SCDMA网工程12个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、集装箱、楼顶增高架、美化天线6种架设方式，其中落地铁塔18个，独管塔6个，楼顶抱杆7个，集装箱2个，楼顶增高架11个，美化天线2个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站6个，GSM900与联通共站2个，TD-SCDMA与联通基站共站1个，其余均为独站；总投资1505万元，其中环保投资88.8万元，占总投资的5.9%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离5.5米；TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离3.0米；GSM900 和TD-SCDMA 共站最大水平防护距离23.5米、垂直防护距离7.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂

家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。n三、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐

许可机关： 河南省环境保护厅

审核类型： 普通

| 行政许可

行政许可决定书文号： 豫环审〔2013〕221号　　第 32 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站197个（其中GSM网工程120个，TD-SCDMA网工程77个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、楼顶增高架4种架设方式，其中落地铁塔117个，独管塔12个，楼顶抱杆56个，楼顶增高架12个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、10瓦，TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站88个，GSM900与联通基站共站3个，GSM900、TD-SCDMA与电信基站共站1个，其余均为独站；总投资7985.5万元，其中环保投资295万元，占总投资的3.69%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900（10W）单站最大水平防护距离13米、垂直防护距离3.0米；GSM900（20W）单站最大水平防护距离23米、垂直防护距离5.5米； GSM900（10W）和TD-SCDMA 共站最大水平防护距离20米、垂直防护距离5.0米；GSM900（20W）和TD-SCDMA 共站最大水平防护距离28米、垂直防护距离6.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉

许可机关： 河南省环境保护厅

审核类型： 普通

| 行政许可

行政许可决定书文号： 豫环审〔2013〕219号　　第 33 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站467个（其中GSM网工程335个，TD-SCDMA网工程132个），其天线类型分为定向型和全向型,定向型天线采用落地铁塔、独管塔、楼顶抱杆、楼顶增高架、室内分布5种架设方式，全向型天线采用室内分布架设，其中落地铁塔336个，独管塔17个，楼顶抱杆37个，楼顶增高架19个，室内分布58个，并建设相应配套设施。基站设备标称发射功率GSM网为2瓦、20瓦、30瓦，TD-SCDMA网为20瓦。GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站43个，GSM900与联通共站2个，GSM900与GSM1800共站24个， GSM900与GSM1800、TD-SCDMA基站共站2个，其余均为独站；总投资20055.3万元，其中环保投资881.4万元，占总投资的4.39 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900（室分）单站最大水平防护距离2.5米、垂直防护距离0.5米；GSM900单站最大水平防护距离27.4米、垂直防护距离5.5米；TD-SCDMA单站最大水平防护距离19.9米、垂直防护距离5.0米；GSM900 和TD-SCDMA 共站最大水平防护距离29.9米、垂直防护距离7.0米；GSM900和联通共站最大水平防护距离33.6米、垂直防护距离6.5米；GSM900 和GSM1800 共站最大水平防护距离29.2米、垂直防护距离6.0米；GSM900 和GSM1800、TD-SCDMA 共站最大水平防护距离35.4米、垂直防护距离7.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕230号　　第 34 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站103个（其中GSM网工程76个，TD-SCDMA网工程27个），其天线类型全部为定向型；采用落地铁塔，独管塔，楼顶抱杆，楼顶增高架4种架设方式，其中落地铁塔45个，独管塔16个，楼顶抱杆8个

，楼顶增高架34个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦，TD-SCDMA网为12瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，其中GSM 网独站9 个，TD-SCDMA 网独站11 个；GSM900 与GSM1800 共站1个，GSM900 与TD-SCDMA 共站28 个，GSM900、GSM1800、TD-SCDMA 共站53个；总投资3385万元，其中环保投资145万元，占总投资的4.28%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单独站最大水平防护距离18米、垂直防护距离4.5米，TD-SCDMA单独站最大水平防护距离15米、垂直防护距离3.0米；GSM900与GSM1800共站情况下最大水平防护距离23.5米、垂直防护距离5.5米，GSM900与TD-SCDMA共站情况下最大水平防护距离27米、垂直防护距离6.5米，GSM900、GSM1800与TD-SCDMA共站情况下最大水平防护距离31米、垂直防护距离7.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。 n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕226号　　第 35 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站232个（其中GSM网工程168个，TD-SCDMA网工程64个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、楼顶增高架、美化天线5种架设方式，其中落地铁塔103个，独管塔39个，楼顶抱杆13个，楼顶增高架60个，美化天线17个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站48个，GSM900与GSM1800共站23个，GSM900与联通共站41个，GSM900与电信基站共站11个，TD-SCDMA与联通共站1个，其余均为独站；总投资16079万元，其中环保投资1091.8万元，占总投资的6.79 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离4.5米；GSM900 和TD-SCDMA 共站最大水平防护距离21.6米、垂直防护距离5.0米；TD-SCDMA 和联通共站最大水平防护距离26.9米、垂直防护距离5.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府

和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕235号　　第 36 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站103个（其中GSM网工程81个，TD-SCDMA网工程22个），其天线类型为定向型；采用落地铁塔、楼顶抱杆、楼顶增高架、美化天线4种架设方式，其中落地铁塔62个，楼顶抱杆1个，楼顶增高架34个，美化天线6个，并建设相应配套设施；基站设备标称发射功率GSM网为40瓦、TD-SCDMA网为9瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站31个，GSM900与联通共站2个，GSM900与GSM1800、TD-SCDMA基站共站5个，其余均为独站；总投资3296万元，其中环保投资152.6万元，占总投资的4.63%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离29.8米、垂直防护距离6.5米；TD-SCDMA单站最大水平防护距离15.0米、垂直防护距离2.5米；GSM900 和TD-SCDMA 共站最大水平防护距离33.4米、垂直防护距离8.0米；GSM900 和GSM1800、TD-SCDMA 共站最大水平防护距离44.8米、垂直防护距离10.0米；GSM900 和联通共站最大水平防护距离36.6米、垂直防护距离6.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕220号　　第 37 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站479个（其中GSM网工程289个，TD-SCDMA网工程190个），其天线类型分为定向型和全向型；定向型天线采用落地铁塔、独管塔,楼顶抱杆,楼顶增高架,美化天线5种架设方式，全向型天线采用室内分布架设,其中落地铁塔275个,独管塔14个,楼顶抱杆46个,楼顶增高架120个，美化天线14个，室内分布120个,并建设相应配套设施；基站设备标称发射功率GSM网为20瓦,TD-SCDMA网为12瓦，GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，其中GSM900和TD-SCDMA共址65个； GSM900与GSM1800共址81个；GSM900基站与联通共址9个；GSM900 基站与电信共址7个；总投资9911.9万元，其中环保投资527.3万元，占总投资的5.32%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900独站最大水平防护距离18米、垂直防护距离4.5米；GSM1800独站最大水平防护距离15米、垂直防护距离3.5米；TD-SCDMA独站最大水平防护距离15.4米、垂直防护距离3.5米；GSM900与GSM1800共站情况下最大水平防护距离23.2米、垂直防护距离5.5米，GSM900与TD-SCDMA共站情况下最大水平防护距离23.5米、垂直防护距离5.5米，GSM900、GSM1800与TD-SCDMA共站情况下最大水平防护距离27.9米、垂直防护距离7.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕227号　　第 38 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站329个（其中GSM网工程209个，TD-SCDMA网工程120个），其天线类型为定向型；采用落地铁塔、楼顶抱杆、楼

顶增高架、美化天线4种架设方式，其中落地铁塔169个，楼顶抱杆3个，楼顶增高架149个，美化天线8个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为9瓦；GSM900上行发射频段分别为890～909兆赫兹，下行发射频段分别为935～954兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站164个，GSM900与GSM1800共站45个，GSM900与TD-SCDMA、联通共站1个，其余均为独站；总投资11354.33万元，其中环保投资470.5万元，占总投资的4.14 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离21.2米、垂直防护距离3.5米； TD-SCDMA单站最大水平防护距离10.7米、垂直防护距离2.0米；GSM900 和TD-SCDMA 共站最大水平防护距离23.7米、垂直防护距离4.0米；GSM900 和GSM1800 共站最大水平防护距离27.6米、垂直防护距离4.5米；GSM900 和GSM1800、TD-SCDMA 共站最大水平防护距离29.4米、垂直防护距离5.0米； GSM900 和GSM1800、TD-SCDMA、联通共站最大水平防护距离38.1米、垂直防护距离6.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕214号　　第 39 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站227个（GSM 网工程147个，TD-SCDMA 网工程80个），其天线类型分为定向型和全向型；定向型天线采用落地铁塔，独管塔，楼顶抱杆，楼顶增高架4种架设方式，全向型天线采用室内分布架设，其中落地铁塔66个，独管塔4个，楼顶抱杆31个，楼顶增高架89个，室内分布37个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦，TD-SCDMA网为12/2瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，GSM900与GSM1800共址21个；GSM900与GSM1800、TD-SCDMA共址32个；GSM900与TD-SCDMA 共址93个；GSM900与TD-SCDMA、联通共址1个；GSM900 与TD-SCDMA、电信共址1个；总投资17439.8万元，其中环保投资640.2万元，占总投资的3.67%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900独站最大水平防护距离17.8米、

垂直防护距离3.5米； TD-SCDMA(室分)独站最大水平防护距离2.2米、垂直防护距离0.5米；GSM900与GSM1800共站情况下最大水平防护距离23.2米、垂直防护距离5.0米，GSM900与TD-SCDMA共站情况下最大水平防护距离24.8米、垂直防护距离5.0米，GSM900、GSM1800与TD-SCDMA共站情况下最大水平防护距离29.0米、垂直防护距离6.0米，GSM900、TD-SCDMA与联通共站情况下最大水平防护距离35.3米、垂直防护距离7.0米，GSM900、TD-SCDMA与电信共站情况下最大水平防护距离35.3米、垂直防护距离7.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕237号　　第 40 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站53个（其中GSM网工程41个，TD-SCDMA网工程12个），其天线类型分为定向型和全向型；定向型天线采用落地铁塔,独管塔,楼顶抱杆,楼顶增高架,美化天线5种架设方式，全向型天线采用室内分布架设,其中落地铁塔30个,独管塔2个,楼顶抱杆13个,楼顶增高架4个，美化天线2个，室内分布2个,并建设相应配套设施；基站设备标称发射功率GSM网为20瓦,TD-SCDMA网为12/2瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，其中GSM900、GSM1800 与TD-SCDMA 共址12个, GSM900 与联通 共址2个；GSM 与TD-SCDMA 共址8个；总投资1588.12万元，环保投资100.5万元，占总投资的6.3%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离19.9米、垂直防护距离3.5米；TD-SCDMA单站最大水平防护距离17.3米、垂直防护距离2.5米；GSM与TD-SCDMA共站情况下最大水平防护距离24.8米、垂直防护距离3.5米；GSM900、GSM1800与TD-SCDMA共站情况下最大水平防护距离29.0米、垂直防护距离5.0米,在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。 n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕223号　　第 41 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站525个（其中GSM网工程359个，TD-SCDMA网工程166个），其天线类型分为定向型和全向型；定向型天线采用落地铁塔、独管塔、集装箱、楼顶抱杆、楼顶增高架、美化天线6种架设方式，全向型天线采用室内分布架设，其中落地铁塔260个，独管塔7个，集装箱3个，楼顶抱杆140个，楼顶增高架51个，美化天线22个，室内分布42个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12/2瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站33个，GSM1800与TD-SCDMA共站86个，GSM900与GSM1800共站86个，GSM900与电信基站共站1个，GSM900与联通共站5个，TD-SCDMA与电信基站共站4个，TD-SCDMA与联通基站共站1个，其余均为独站；总投资16800万元，其中环保投资873.6万元，占总投资的5.2 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离3.5米；GSM1800单站最大水平防护距离21.1米、垂直防护距离4.0米；TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离5.0米；TD-SCDMA（室分）单站最大水平防护距离4.0米、垂直防护距离0.5米；GSM900 和GSM1800 共站最大水平防护距离23.2米、垂直防护距离3.0米；GSM900 和TD-SCDMA 共站最大水平防护距离23.2米、垂直防护距离7.0米；GSM1800 和TD-SCDMA 共站最大水平防护距离22.9米、垂直防护距离4.0米； GSM900 和GSM1800、TD-SCDMA 共站最大水平防护距离32.6米、垂直防护距离6.5米； TD-SCDMA和联通共站最大水平防护距离24.8米、垂直防护距离3.5米，在此范围内设立为辐射防护

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕223号　　第 42 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站195个（其中GSM网工程89个，TD-SCDMA网工程106个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、楼顶增高架4种架设方式，其中落地铁塔52个，独管塔1个，楼顶抱杆41个，楼顶增高架101个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12瓦；GSM900天线上行发射频段分别为890～909兆赫兹，下行发射频段分别为935～954兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站123个，GSM900独站49个， GSM900与GSM1800共站12个，GSM900、GSM1800、TD-SCDMA共站7个，GSM900与电信共站1个，GSM900与联通共站1个，TD-SCDMA与电信共站1个，TD-SCDMA与联通共站1个；总投资5708.7万元，其中环保投资365.5万元，占总投资的6.4%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离3.5米；GSM900和TD-SCDMA 共站最大水平防护距离23.5米、垂直防护距离5.0米，GSM900 和GSM1800 共站最大水平防护距离23.2米、垂直防护距离5.0米，GSM900、GSM1800和TD-SCDMA 共站最大水平防护距离27.9米、垂直防护距离6.0米，GSM900和联通共站最大水平防护距离25.1米、垂直防护距离5.0米， TD-SCDMA和电信共站最大水平防护距离23.5米、垂直防护距离3.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕224号　　第 43 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站120个（其中GSM网工程50个，TD-CDMA网工程70个），其天线类型分为定向型和全向型；定向型天线采用落地铁塔,独管塔,楼顶抱杆,楼顶增高架, 4种架设方式，全向型天线采用室内分布架设,其中落地铁塔3个,独管塔5个,楼顶抱杆46个,楼顶增高架37个，室内分布29个,并建设相应配套设施；基站设备标称发射功率GSM网为27/2瓦,TD-SCDMA网为12瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，GSM900和TD-SCDMA共址67个；TD-SCDMA与联通共址1个；总投资6718.2万元，其中环保投资249.24万元，占总投资的3.71%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900独站最大水平防护距离分别为21.9米、垂直防护距离分别为5.5米； GSM1800独站最大水平防护距离16.4米、垂直防护距离2.0米；TD-SCDMA独站最大水平防护距离30.8米、垂直防护距离9.0米；

GSM900与TD-SCDMA共站情况下最大水平防护距离37.8米、垂直防护距离13.0米，TD-SCDMA与联通共站情况下最大水平防护距离39.7米、垂直防护距离11.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置等措施，不得施工扰民。项目建设中破坏的农

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕217号　　第 44 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站477个（其中GSM网工程353个，TD-SCDMA网工程124个），其天线类型全部为定向型；采用美化塔，落地铁塔，独管塔，楼顶抱杆，楼顶增高架，集装箱，楼顶美化天线7种架设方式，其中美化塔32个，落地铁塔209，独管塔20个，楼顶抱杆30个，楼顶增高架142个，集装箱13个，楼顶美化天线31个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦,TD-SCDMA网为12瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，其中GSM900与GSM1800共站7个, GSM1800与TD-SCDMA共站8个, GSM900与联通共站4个, GSM1800与联通共站1个, GSM900与TD-SCDMA共站96个,其余均为独站；总投资13420万元，环保投资650万元，占总投资的4.84%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离4.5米；GSM1800单站最大水平防护距离15.0米、垂直防护距离3.5米；TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离2.5米；GSM900与GSM1800共站情况下最大水平防护距离23.3米、垂直防护距离7.0米，GSM1800与TD-SCDMA共站情况下最大水平防护距离21.5米、垂直防护距离7.5米，GSM900与联通共站情况下最大水平防护距离25.2米、垂直防护距离6.0米，GSM1800与联通共站情况下最大水平防护距离23.3米、垂直防护距离5.0米，GSM900与TD-SCDMA共站情况下最大水平防护距离23.6米、垂直防护距离6.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕222号　　第 45 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站268个（其中GSM网工程252个，TD-SCDMA网工程16个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、楼顶增高架、美化天线5种架设方式，其中落地铁塔134个，独管塔80个，楼顶抱杆12个，楼顶增高架28个，美化天线14个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦，TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM与TD-SCDMA共站23个，GSM900与联通、电信基站共站30个，GSM900与GSM1800共站1个，其余均为独站；总投资7879.2万元，其中环保投资465.9万元，占总投资的5.91 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离3.5米； GSM900 和TD-SCDMA 共站最大水平防护距离24.1米、垂直防护距离5.5米；GSM900 和GSM1800 共站最大水平防护距离23.2米、垂直防护距离5.0米；GSM900 和联通共站最大水平防护距离23.2米、垂直防护距离2.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕238号　　第 46 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站46个（其中GSM网工程30个，TD-SCDMA网工程16个），其天线类型全部为定向型；采用落地铁塔，楼顶增高架，2种

架设方式，其中落地铁塔26个，楼顶增高架20个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦,TD-SCDMA网为12瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，其中GSM与TD-SCDMA 共址16个； GSM900、GSM1800与TD-SCDMA共址4个,总投资1328.88万元，环保投资60.95万元，占总投资的4.6%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离21.1米、垂直防护距离3.5米；GSM与TD-SCDMA共站情况下最大水平防护距离24.4米、垂直防护距离4.0米；GSM900、GSM1800与TD-SCDMA共站情况下最大水平防护距离27.0米、垂直防护距离4.5米,在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。n三、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测，发现问题及时采取措施加以解决。n四、

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕225号　　第 47 条

许可有效期： ——

许可决定日期： 2013-05-08

许可截止日期： ——

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站1041个（其中GSM网工程699个，TD-SCDMA网工程342个），其天线类型为定向型；采用落地铁塔、楼顶抱杆、楼顶增高架、美化天线4种架设方式，其中落地铁塔528个，楼顶抱杆12个，楼顶增高架440个，美化天线61个，并建设相应配套设施；基站设备标称发射功率GSM网为40瓦、TD-SCDMA网为9瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站273个，GSM900与电信或联通共站14个，GSM1800与TD-SCDMA共站27个， GSM1800与其他GSM共站6个， TD-SCDMA与电信或联通基站共站2个，GSM900与GSM1800、TD-SCDMA基站共站15个，其余均为独站；总投资32250万元，其中环保投资1280.8万元，占总投资的3.97%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离29.8米、垂直防护距离8.0米；TD-SCDMA单站

最大水平防护距离15.0米、垂直防护距离2.0米； GSM900 和TD-SCDMA 共站最大水平防护距离39.4米、垂直防护距离11.0米；GSM1800 和TD-SCDMA 共站最大水平防护距离31.7米、垂直防护距离3.5米； GSM900 和GSM1800、TD-SCDMA 共站最大水平防护距离40.5米、垂直防护距离8.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕218号　　第 48 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站145个（其中GSM网工程105个，TD-SCDMA网工程40个），其天线类型全部为定向型；采用落地铁塔,独管塔,楼顶抱杆,楼顶增高架4种架设方式，其中落地铁塔68个,独管塔14个,楼顶抱杆33个,楼顶增高架30个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦,TD-SCDMA网为12瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，其中GSM网独站69个；TD-SCDMA 网独站1个；GSM900、GSM1800共站1个；GSM900、TD-SCDMA 共站42 个；GSM900、GSM1800、TD-SCDMA 共站23个；GSM900、联通共站6 个；GSM900、GSM1800、TD-SCDMA、联通共站2 个；GSM900、GSM1800、TD-SCDMA、电信共站1 个；GSM900、电信共站1 个；总投资4764.6万元，其中环保投资185万元，占总投资的3.88%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900独站最大水平防护距离18米、垂直防护距离4.0米；TD-SCDMA独站最大水平防护距离16米、垂直防护距离3.5米；GSM900与GSM1800共站情况下最大水平防护距离26米、垂直防护距离5.5米，GSM900与TD-SCDMA共站情况下最大水平防护距离24米、垂直防护距离5.5米，GSM900、GSM1800与TD-SCDMA共站情况下最大水平防护距离28米、垂直防护距离6.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕229号　　第 49 条

许可有效期： ——

许可决定日期： 2013-05-08

许可截止日期： ——

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站119个（其中GSM网工程106个，TD-SCDMA网工程13个），天线类型为定向型；采用美化塔、落地铁塔、独管塔、楼顶抱杆、楼顶增高架、楼顶美化天线6种架设方式，其中美化塔4个，落地铁塔58个，独管塔12个，楼顶抱杆7个，楼顶增高架30个，楼顶美化天线8个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900独站92个,TD-SCDMA独站2个,GSM900与TD-SCDMA共站17个，GSM1800与TD-SCDMA共站3个；总投资3350万元，其中环保投资160万元，占总投资的4.78%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离5.0米；GSM1800单站最大水平防护距离15.0米、垂直防护距离4.5米；TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离2.5米；GSM900 和TD-SCDMA 共站最大水平防护距离23.6米、垂直防护距离6.5米；GSM1800 和TD-SCDMA共站最大水平防护距离21.5米、垂直防护距离5.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕229号　　第 50 条

许可有效期： ——

许可决定日期： 2013-05-08

许可截止日期： ——

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站282个（其中GSM网工程241个，TD-SCDMA网工程41个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、楼顶增高架、美化天线5种架设方式，其中落地铁塔144个，独管塔14个，楼顶抱杆58个，楼顶增高架16个，美化天线50个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦，TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站48个，GSM900与GSM1800共站23个，GSM900与联通共站41个，GSM900与电信共站11个，其余均为独站；总投资17241.8万元，其中环保投资1015.5万元，占总投资的5.89 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离3.5米；TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离2.0米；GSM900 和TD-SCDMA 共站最大水平防护距离23.5米、垂直防护距离5.0米；GSM900 和GSM1800 共站最大水平防护距离27.6米、垂直防护距离5.0米；GSM900 和GSM1800、TD-SCDMA 共站最大水平防护距离31.6米、垂直防护距离6.0米；在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕215号　　第 51 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站1030个（其中GSM网工程666个，TD-SCDMA网工程364个），其天线类型全部为定向型；采用落地铁塔，独管塔，楼顶抱杆，楼顶增高架4种架设方式，其中落地铁塔187个，独管塔147个，楼顶抱杆447个，楼顶增高架249个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦，TD-SCDMA网为12瓦；GSM900、GSM1800基站天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA基站天线上行和下行发射频段均为2010～2025兆赫兹，GSM900和GSM1800共站9个；GSM900和TD-SCDMA共站109个；GSM1800和TD-SCDMA共站39个；GSM900、GSM1800和TD-SCDMA共站28个；GSM和联通共站22个；TD-SCDMA和联通共站8个；GSM和电信共站8个；GSM、TD-SCDMA和联通共站2个；GSM、TD-SCDMA 和电信共站1个；总投资19826.7万元，其中环保投资763.4万元，占总投资的3.85%。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心

，GSM900独站最大水平防护距离17.8米、垂直防护距离6.0米；GSM1800独站最大水平防护距离14.9米、垂直防护距离3.5米；TD-SCDMA独站最大水平防护距离16.3米、垂直防护距离6.5米；GSM900与GSM1800共站情况下最大水平防护距离23.2米、垂直防护距离5.0米，GSM900与TD-SCDMA共站情况下最大水平防护距离24.1米、垂直防护距离9.0米，GSM1800与TD-SCDMA共站情况下最大水平防护距离22.1米、垂直防护距离7.5米;GSM900、GSM1800与TD-SCDMA共站情况下最大水平防护距离28.4米、垂直防护距离6.0米，GSM与联通共站情况下最大水平防护距离30.7米、垂直防护距离7.5米; TD-SCDMA与联通共站情况下最大水平防护距离29.9米、垂直防护距离7.0米; GSM与电信共站情况下最大水平防

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕216号　　第 52 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站247个（其中GSM网工程152个，TD-SCDMA网工程95个），其天线类型为定向型；采用落地铁塔、独管塔、楼顶抱杆、集装箱、楼顶增高架、美化天线6种架设方式，其中落地铁塔97个，独管塔34个，楼顶抱杆37个，集装箱9个，楼顶增高架59个，美化天线11个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站81个，GSM900与联通共站9个，TD-SCDMA与电信基站共站3个，其余均为独站；总投资8082万元，其中环保投资476.8万元，占总投资的5.9 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离5.5米；TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离3.0米；GSM900 和TD-SCDMA 共站最大水平防护距离23.5米、垂直防护距离5.5米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。n三、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行

许可机关： 河南省环境保护厅

审核类型： 普通

行政许可

行政许可决定书文号： 豫环审〔2013〕213号 第 53 条

许可有效期： — —

许可决定日期： 2013-05-08

许可截止日期： — —

许可内容： 一、项目建设内容和总体要求n本期项目共建设基站1847个（其中GSM网工程488个，TD-SCDMA网工程1359个），其天线类型为定向型；采用落地铁塔、楼顶抱杆、楼顶增高架、美化天线4种架设方式，其中落地铁塔506个，楼顶抱杆351个，楼顶增高架883个，美化天线107个，并建设相应配套设施；基站设备标称发射功率GSM网为20瓦、TD-SCDMA网为12瓦；GSM900、GSM1800天线上行发射频段分别为890～909兆赫兹、1710～1725兆赫兹，下行发射频段分别为935～954兆赫兹、1805～1820兆赫兹，TD-SCDMA天线上下行发射频段均为2010～2025兆赫兹，其中GSM900与TD-SCDMA共站109个，TD-SCDMA与联通共站2个，其余均为独站；总投资51816万元，其中环保投资2404万元，占总投资的4.64 %。n以上项目在落实《报告书》提出的各项环境保护措施后，环境不利影响能够得到有效控制，满足相关标准要求。因此，我厅同意你单位按照报告书所列项目的内容、地点及采取的环境保护措施进行建设。n二、项目建设和运营中应重点做好的工作n1、设立辐射防护区，以基站天线为中心，GSM900单站最大水平防护距离17.8米、垂直防护距离5.0米；TD-SCDMA单站最大水平防护距离15.4米、垂直防护距离5.0米；GSM900 和TD-SCDMA 共站最大水平防护距离23.5米、垂直防护距离6.0米，在此范围内设立为辐射防护区域，设置警示标志，限制公众在辐射防护区域内的活动。将本批项目的辐射防护区域、电磁辐射功率密度控制标准（8微瓦/平方厘米）及防护要求告知当地政府和相关部门，确保在此区域内不得新建医院、学校、居民住宅等环境敏感建筑。n2、为加强特殊敏感人群的保护，基站建设应科学规划，合理选址，设立安全防护距离，确保环境和公众安全。n3、采取降噪措施，保证机房等设施产生的噪声达到标准要求。n4、基站运行过程中产生的废旧蓄电池应由有资质的厂家回收处理，不得随意丢弃，避免造成环境污染。n5、落实施工期各项污染防治措施，采取有效防尘、降噪和施工弃渣处置措施，不得施工扰民。项目建设中破坏的农田和林地，应及时恢复。n6、加强对公众电磁辐射知识宣传，妥善解决基站投诉问题，确保社会稳定。n三、你单位应建立环保管理和监测制度，定期对基站周围和环境保护目标进行相关的电磁辐射和噪声监测，发现问题及时采取措施加以解决

许可机关： 河南省环境保护厅

审核类型： 普通

三、诚实守信相关荣誉信息 (共 4 条)

纳税信用A级纳税人

纳税人名称： 中国移动通信集团河南有限公司 第 1 条

纳税人识别号： 91410000719172532Q

评价年度： 2022

数据来源： 国家税务总局

| 纳税信用A级纳税人 第 2 条

纳税人名称： 中国移动通信集团河南有限公司

纳税人识别号： 9141000071917 25

评价年度： 2021

数据来源： 国家税务总局

| 纳税信用A级纳税人 第 3 条

纳税人名称： 中国移动通信集团河南有限公司

纳税人识别号： 9141000071917 2532Q

评价年度： 2020

数据来源： 国家税务总局

| 纳税信用A级纳税人 第 4 条

纳税人名称： 中国移动通信集团河南有限公司

纳税人识别号： 9141000071917 2532Q410105719172532

评价年度： 2016

数据来源： 国家税务总局

四、严重失信信息 (共 0 条)

查询期内无相关记录

五、经营（活动）异常名录（状态）信息 (共 0 条)

查询期内无相关记录

六、信用承诺信息 (共 73 条)

企业信用承诺信息

第 1 条

承诺编码：	410700202109 29G5 772
承诺类型：	行业自律型
承诺事由：	全省房屋建筑和市政基础设施工程项目招标投标活动承诺书
承诺内容：	<h2 style="text-align:center" >全省房屋建筑和市政基础设施工程项目招标投标活动承诺书</h2> 我单位承诺,在延津县应急指挥平台硬件建设项目项目招投标活动中,自觉遵守《中华人民共和国招标投标法》、《中华人民共和国招标投标法实施条例》、河南省实施《中华人民共和国招标投标法》办法等招标投标相关法律、法规和制度规定,如有违反,愿承担相关法律责任。 投标人： 中国移动通信集团河南有限公司 承诺人（法人代表）： 杨威 日期： 2021年09月29日
承诺作出日期：	2021-09-29
承诺履行状态：	全部履行
承诺受理单位：	新乡市公共资源交易管理中心
承诺受理单位统一社会信用代码：	124107006716746398

企业信用承诺信息

第 2 条

承诺类型：	证明事项型
承诺事由：	投标信誉承诺书
承诺作出日期：	2021-12-26
承诺受理单位：	新乡市公共资源交易管理中心
承诺履行状态：	— —

企业信用承诺信息

承诺类型：	行业自律型	第 3 条
承诺事由：	行业自律	
承诺作出日期：	2021-09-14	
承诺受理单位：	焦作市发展和改革委员会	
承诺履行状态：	一一履约	

企业信用承诺信息

承诺编码：	410700202109 29G14924	第 4 条
承诺类型：	主动型	
承诺事由：	资料真实性承诺书	
承诺内容：	资料真实性承诺书 延津县应急管理局: 我方在此声明,我方所提供的以上资料均真实和准确。我方保证上述信息的真实和准确,并愿意承担因我方就此弄虚作假所引起的一切法律后果。 特此承诺。 投标人:中国移动通信集团河南有限公司 法定代表人:杨威 日期：2021-09-29 	
承诺作出日期：	2021-09-29	
承诺履行状态：	全部履行	
承诺受理单位：	新乡市公共资源交易管理中心	
承诺受理单位统一社会信用代码：	124107006716746398	

企业信用承诺信息

承诺编码： 41070020211112G79680 第 5 条

承诺类型： 证明事项型

承诺事由： 投标信誉承诺书

承诺内容： <p style="text-indent:2em;"><table border="0" cellpadding="0" cellspacing="0" width="629" style="width:472pt;" class="ke-zeroborder"><tbody><tr><td height="187" class="xl65" width="629"><h1 style="text-align:center;">信誉承诺书</h1>获嘉县卫生健康委员会:
   我方在此承诺，我方信誉良好，现阶段没有处于被责令停产、停业，或者投标资格被取消，无骗取中标或者严重违约或重大工程质量安全生产事故等问题；我方承诺上述信息的真实和准确，一经发现失实我方愿意无条件自动放弃中标资格。
特此承诺
   投标人：中国移动通信集团河南有限公司
   法定代表人：赵超
   日期：2021-11-12</td></tr></tbody></table></p>

承诺作出日期： 2021-11-12

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺编码： 41070020210907F86181 第 6 条

承诺类型： 证明事项型

承诺事由： 不拖欠农民工工资承诺书

承诺内容： <h1 style="text-align:center;">不拖欠农民工工资承诺书</h1>延津县应急管理局:
   若我公司中标,我公司承诺在(项目名称)施工期间不拖欠农民工工资,建立支付农民工工资专项保证金。
   我公司保证不拖欠农民工工资,一定将农民工工资足额直接发放到农民工手中,并保证将每月工资发放表及时上报给贵公司,并保证资料的真实有效性;如有虚假和不报的情况发生,我公司愿意接受贵单位的处罚。
<span style="font-

family:FangSong_GB2312;font-size:16px;">   投标人：中国移动通信集团河南有限公司
   法定代表人：杨威
   日期：2021年09月07日

承诺作出日期： 2021-09-07

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107000071674 6398

企业信用承诺信息

第 7 条

承诺类型： 证明事项型

承诺事由： 不拖欠农民工工资承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 8 条

承诺类型： 证明事项型

承诺事由： 项目经理无在建承诺书

承诺作出日期： 2021-12-26

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 9 条

承诺编码： 41070020211122G54057

承诺类型： 行业自律型

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺内容： <h2 style="text-align:center;">全省房屋建筑和市政基础设施工程项目招标投标活动承诺书</h2>   我单位承诺,在获嘉县医共体信息化平台服务项目二次项目招标活动中,自觉遵守《中华人民共和国招标投标法》、《中华人民共和国招标投标法实施条例》、河南省实施《中华人民共和国招标投标法》办法等招标投标相关法律、法规和制度规定,如有违反,愿承担相关法律责任。
   投标人： 中国移动通信集团河南有限公司
   承诺人（法人代表）： 赵超
   日期： 2021年11月22日

承诺作出日期： 2021-11-22

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺类型： 证明事项型　　第 10 条

承诺事由： 不拖欠农民工工资承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 行业自律型　　第 11 条

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 证明事项型 第 12 条

承诺事由： 申请办理投资项目备[illegible]

承诺作出日期： 2020-09-14

承诺受理单位： 河南省发展和改革委员会

承诺履行状态： — —

企业信用承诺信息

承诺类型： 证明事项型 第 13 条

承诺事由： 申报项目

承诺作出日期： 2022-04-28

承诺受理单位： 河南省发展和改革委员会

承诺履行状态： — —

企业信用承诺信息

承诺编码： 410700202109 29G62235 第 14 条

承诺类型： 证明事项型

承诺事由： 投标信誉承诺书

承诺内容： <p style="text-indent:2em;"><table border="0" cellpadding="0" cellspacing="0" width="629" style="width:472pt;" class="ke-zeroborder"><tbody><tr><td height="187" class="xl65" width="629"> <h1 style="text-align:center;">信誉承诺书</h1>延津县应急管理局:
   我方在此承诺，我方信誉良好，现阶段没有处于被责令停产、停业，或者投标资格被取消，无骗取中标或者严重违约或者重大工程质量安全生产事故等问题；我方承诺上述信息的真实和准确，一经发现失实我方愿意无条件自动放弃中标资格。
特此承诺
   投标人：中国移动通信集团河南有限公司
   法定代表人：杨威
   日期：2021-09-29</u></tbody></table></p>

承诺作出日期： 2021-09-29

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺编码： 41070020210929H04612 第 15 条

承诺类型： 证明事项型

承诺事由： 项目经理无在建承诺书

承诺内容： <h1 style="text-align:center;">项目经理无在建承诺书</h1>延津县应急管理局:
   我方在此声明,我方拟派往延津县应急指挥平台硬件建设项目(以下简称“本工程”)的项目经理在本项目报名之日起不再担任其他正在施工建设项目的项目经理或项目负责人。我方保证上述信息的真实和准确,如果发现并证实项目经理有在建工程,我方愿意自动放弃中标资格。
 特此承诺。
   投标人：中国移动通信集团河南有限公司
   法定代表人：杨威
   日期：2021年09月29日

承诺作出日期： 2021-09-29

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺类型： 主动型 第 16 条

承诺事由： 资料真实性承诺书

承诺作出日期： 2021-12-28

承诺受理单位： 新乡市公共资源交易[illegible]心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 证明事项型 第 17 条

承诺事由： 申请办理投资项目备案

承诺作出日期： 2020-09-14

承诺受理单位： 河南省发展和改革委员会

承诺履行状态： — —

企业信用承诺信息

承诺类型： 主动型 第 18 条

承诺事由： 为维护市场公平竞争，营造诚实守信的公共资源交易环境，本申请人自愿加入“鹤壁市公共资源交易中心会员库”（以下简称会员库），自愿将本申请人相关信息予以登记，并郑重承诺如下：一、本申请人提交并在信息库的相关信息均真实有效，提交的材料无任何伪造、修改、虚假成份，材料所述内容均为本申请人真实拥有。若违反本承诺，一经查实，本申请人自愿退出所有正在鹤壁市公共资源交易中心进行的交易项目并取消会员资格，愿意接受公开通报及有关处罚，并承担相应法律责任；二、本申请人自愿将我方入库信息在鹤壁市公共资源交易中心网站公开，并在评标结果公示时对外公布，接受社会监督。因我方自行填报信息的错误、缺项造成的后果由我方自行承担；三、本申请人今后将认真、及时维护和更新诚信库中与本申请人有关的内容，如未能及时维护和更新，自愿承担由此造成的一切后果及法律责任。

承诺作出日期： 2021-03-25

承诺受理单位： 鹤壁市公共资源交易中心

承诺履行状态： — —

企业信用承诺信息

承诺编码： 410122201901053567 23 第 19 条

承诺类型： 主动型

承诺事由： 自愿作出承诺

承诺内容： 承诺:申请材料真实有效齐全且符合法定形式

承诺作出日期： 2019-01-05

承诺履行状态： 全部履行

承诺受理单位： 中牟县人民防空办公室

承诺受理单位统一社会信用代码： 114101227765133487

企业信用承诺信息

承诺编码： 41070020211112G08162 第 20 条

承诺类型： 主动型

承诺事由： 资料真实性承诺书

承诺内容： <h1 style="text-align:center;">资料真实性承诺书</h1>获嘉县卫生健康委员会:
   我方在此声明,我方所提供的以上资料均真实和准确。我方保证上述信息的真实和准确,并愿意承担因我方就此弄虚作假所引起的一切法律后果。
特此承诺。
   投标人:中国移动通信集团河南有限公司
   法定代表人:赵超
   日期：2021-11-12

承诺作出日期： 2021-11-12

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

第 21 条

承诺编码： 410700202109[illegible]

承诺类型： 行业自律型

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺内容： <h2 style="text-align:center;">全省房屋建筑和市政基础设施工程项目招标投标活动承诺书</h2>   我单位承诺,在延津县应急指挥平台硬件建设项目项目招投标活动中,自觉遵守《中华人民共和国招标投标法》、《中华人民共和国招标投标法实施条例》、河南省实施《中华人民共和国招标投标法》办法等招标投标相关法律、法规和制度规定,如有违反,愿承担相关法律责任。
   投标人： 中国移动通信集团河南有限公司
   承诺人（法人代表）： 杨威
   日期： 2021年09月07日

承诺作出日期： 2021-09-07

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

第 22 条

承诺类型： 行业自律型

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 23 条

承诺类型： 主动型

承诺事由： 申请参与公共资源交易活动

承诺作出日期： 2021-10-28

承诺受理单位： 长垣市公共资源交易中心

承诺履行状态： — —

企业信用承诺信息

第 24 条

承诺编码： 410700202109 29G46196

承诺类型： 证明事项型

承诺事由： 不拖欠农民工工资承诺书

承诺内容： <h1 style="text-align:center;">不拖欠农民工工资承诺书</h1>延津县应急管理局:
   若我公司中标,我公司承诺在(项目名称)施工期间不拖欠农民工工资,建立支付农民工工资专项保证金。
   我公司保证不拖欠农民工工资,一定将农民工工资足额直接发放到农民工手中,并保证将每月工资发放表及时上报给贵公司,并保证资料的真实有效性;如有虚假和不报的情况发生,我公司愿意接受贵单位的处罚。
   投标人：中国移动通信集团河南有限公司
   法定代表人：杨威
   日期：2021年09月29日

承诺作出日期： 2021-09-29

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺类型： 证明事项型 第 25 条
承诺事由： 项目经理无在建承诺书
承诺作出日期： 2021-12-26
承诺受理单位： 新乡市公共资源交易管理中心
承诺履行状态： — —

企业信用承诺信息

承诺类型： 主动型 第 26 条
承诺事由： 自愿
承诺作出日期： 2022-01-07
承诺受理单位： 郑州市信息中心
承诺履行状态： — —

企业信用承诺信息

承诺编码： 41088320200806000001 第 27 条
承诺类型： 主动型
承诺事由： 项目备案
承诺内容： 所提供材料真实有效
承诺作出日期： 2020-08-06
承诺履行状态： 全部履行
承诺受理单位： 孟州市发展和改革委员会
承诺受理单位统一社会信用代码： 114108830056971347

企业信用承诺信息

承诺类型： 行业自律型 第 28 条

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 29 条

承诺类型： 行业自律型

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 30 条

承诺类型： 证明事项型

承诺事由： 申请办理投资项目备案

承诺作出日期： 2020-09-14

承诺受理单位： 河南省发展和改革委员会

承诺履行状态： — —

企业信用承诺信息

第 31 条

承诺编码： 41070020211103G95488

承诺类型： 证明事项型

承诺事由： 项目经理无在建承诺书

承诺内容： <h1 style="text-align:center;">项目经理无在建承诺书</h1>延津县产业集聚区管理

委员会:
   我方在此声明,我方拟派往延津县产业集聚区管理委员会智慧化工园区信息平台（一期）建设工程项目(以下简称“本工程”)的项目经理石延勇在本项目报名之日起不再担任其他正在施工建设项目的项目经理或项目负责人。我方保证上述信息的真实和准确,如果发现并证实项目经理有在建工程,我方愿意自动放弃中标资格。
 特此承诺。
   投标人：中国移动通信集团河南有限公司
   法定代表人：张建国
   日 期：2021年11月03日

承诺作出日期： 2021-11-03

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺类型： 主动型　　第 32 条

承诺事由： 主动承诺

承诺作出日期： 2021-08-03

承诺受理单位： 三门峡市发展和改革委员会

承诺履行状态： — —

企业信用承诺信息

承诺类型： 主动型　　第 33 条

承诺事由： 一、 提供给行政部门、行业管理部门、司法部门及行业组 织的所有资料均合法、真实、有效，并对所提供资料的真实性 负责； 二、 遵守国家法律、法规、规章和政策规定，开展生产经 营活动，主动接受行业监管，自愿接受依法开展的日常检查； 三、 若发生违法失信行为，将依照有关法律、法规规章和 政策规定接受处罚，并依法承担相应责任； 四、 自觉接受政府、行业组织、社会公众、新闻舆论的监 督，积极履行社会责任； 五、自愿按照信用信息管理有关要求，将信用承诺信息纳入各级信用信息共享平台，并通过各级信用网站向社会公开。

承诺作出日期： 2021-11-14

承诺受理单位： 国家税务总局信阳市税务局

承诺履行状态： — —

企业信用承诺信息

承诺编码： 410122201706200[illegible]280 第 34 条

承诺类型： 容缺受理型

承诺事由： 参加我县组织的信用承诺活动

承诺内容： 已经知晓政务服务部门告知的全部内容

承诺作出日期： 2017-06-20

承诺履行状态： 全部履行

承诺受理单位： 中牟县发改委

承诺受理单位统一社会信用代码： 11410122747414674K

企业信用承诺信息

承诺编码： 41072120211103C14594 第 35 条

承诺类型： 证明事项型

承诺事由： 投标信誉承诺书

承诺内容： <p style="text-indent:2em;"><table border="0" cellpadding="0" cellspacing="0" width="629" style="width:472pt;" class="ke-zeroborder"><tbody><tr><td height="187" class="xl65" width="629"> <h1 style="text-align:center;">信誉承诺书</h1>延津县产业集聚区管理委员会:
   我方在此承诺，我方信誉良好，现阶段没有处于被责令停产、停业，或者投标资格被取消，无骗取中标或者严重违约或者重大工程质量安全生产事故等问题；我方承诺上述信息的真实和准确，一经发现失实我方愿意无条件自动放弃中标资格。
特此承诺
   投标人：中国移动通信集团河南有限公司
   法定代表人：张建国
   日期：2021-11-03</td></tr></tbody></table></p>

承诺作出日期： 2021-11-03

承诺履行状态： 全部履行

承诺受理单位： 新乡县公共资源交易中心

承诺受理单位统一社会信用代码： 12410721699962368U

企业信用承诺信息

承诺类型： 主动型 第 36 条

承诺事由： 资料真实性承诺书

承诺作出日期： 2021-12-28

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 行业自律型 第 37 条

承诺事由： 申请流通领域

承诺作出日期： 2020-03-24

承诺受理单位： 郑州市发改委

承诺履行状态： — —

企业信用承诺信息

承诺类型： 主动型 第 38 条

承诺事由： 申请参与新乡市公共资源交易招投标活动

承诺作出日期： 2020-09-14

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 39 条

承诺编码：	410700520200907531419
承诺类型：	主动型
承诺事由：	主动作，自愿作出承诺
承诺内容：	确保统计资料的报送及统计调查所需材料，建立健全统计资料的管理制度，杜绝任何违反统计法律和统计调查制度的行为
承诺作出日期：	2020-09-07
承诺履行状态：	全部履行
承诺受理单位：	金水区统计局
承诺受理单位统一社会信用代码：	11410105MB1D66812K

企业信用承诺信息

第 40 条

承诺编码：	410700202111112F87981
承诺类型：	证明事项型
承诺事由：	不拖欠农民工工资承诺书
承诺内容：	不拖欠农民工工资承诺书 获嘉县卫生健康委员会: 若我公司中标,我公司承诺在(项目名称)施工期间不拖欠农民工工资,建立支付农民工工资专项保证金。 我公司保证不拖欠农民工工资,一定将农民工工资足额直接发放到农民工手中,并保证将每月工资发放表及时上报给贵公司,并保证资料的真实有效性;如有虚假和不报的情况发生,我公司愿意接受贵单位的处罚。 投标人：中国移动通信集团河南有限公司 法定代表人：赵超 日期：2021年11月12日
承诺作出日期：	2021-11-12
承诺履行状态：	全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺编码： 410700202109[illegible] 第 41 条

承诺类型： 证明[illegible]型

承诺事由： 投标信誉承诺书

承诺内容： <p style="[illegible]text-indent:[illegible]cm;"><table border="0" cellpadding="0" cellspacing="0" width="629" style="width:472pt;" class="ke-zeroborder"><tbody><tr><td height="187" class="xl65" width="629"> <h1 style="text-align:center;">信誉承诺书</h1>延津县应急管理局:
   我方在此承诺，我方信誉良好，现阶段没有处于被责令停产、停业，或者投标资格被取消，无骗取中标或者严重违约或者重大工程质量安全生产事故等问题；我方承诺上述信息的真实和准确，一经发现失实我方愿意无条件自动放弃中标资格。
特此承诺
   投标人：中国移动通信集团河南有限公司
   法定代表人：杨威
   日期：2021-09-07</td></tr></tbody></table></p>

承诺作出日期： 2021-09-07

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺编码： 41070020211122G15146 第 42 条

承诺类型： 主动型

承诺事由： 资料真实性承诺书

承诺内容： <h1 style="text-align:center;">资料真实性承诺书</h1><span

style="font-family:FangSong_GB2312;font-size:16px;">获嘉县卫生健康委员会:
   我方在此声明,我方所提供的以上资料均真实和准确。
我方保证上述信息的真实和准确,并愿意承担因我方就此弄虚作假所引起的一切法律后果。
特此承诺。

 投标人:中国移动通信集团河南有限公司
   法定代表人:赵超
   日期：2021-11-22

承诺作出日期： 2021-11-22

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺类型： 证明事项型　　第 43 条

承诺事由： 投标信誉承诺书

承诺作出日期： 2021-12-26

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺编码： 410783201707 12A13033　　第 44 条

承诺类型： 行业自律型

承诺事由： 申请参与公共资源交易活动

承诺内容： 为维护公共资源交易当事人的合法权益，营造公平公正的良好交易环境，我单位自愿加

入长垣市公共资源交易中心投标人（供应商、竞买人）主体诚信库（以下简称诚信库），成为注册投标人（供应商、竞买人）会员，并郑重做出如下承诺： 一、我单位提交审核并在诚信库中登记的相关资料信息均真实有效，无任何伪造、修改、虚假成份，材料所述内容均为本申请人真实拥有。若违反本承诺，一经查实，自愿退出所有正在长垣市公共资源交易管理中心进行的交易项目并取消会员资格，愿意接受公开通报及有关处罚并承担相应法律责任。 二、我单位将认真、及时维护和更新诚信库中与我单位有关的内容，如未能及时维护和更新，将自愿承担由此造成的一切后果。 三、我单位未在诚信库中发布的企业信息，一律不作为在参与电子交易项目时有效依据。 四、我单位充分认识到诚信库账号和密码以及数字证书的重要性，将安排专人妥善保管和使用，如因保管不善被盗用，我单位自愿承担相关责任。

承诺作出日期： 2017-07-12

承诺履行状态： 全部履行

承诺受理单位： 长垣市公共资源交易中心

承诺受理单位统一社会信用代码： 12410728592417****

企业信用承诺信息

承诺编码： 410700202111112G60845　　第 45 条

承诺类型： 证明事项型

承诺事由： 项目经理无在建承诺书

承诺内容： <h1 style="text-align:center;">项目经理无在建承诺书</h1>获嘉县卫生健康委员会:
   我方在此声明,我方拟派往获嘉县医共体信息化平台服务项目(以下简称“本工程”)的项目经理在本项目报名之日起不再担任其他正在施工建设项目的项目经理或项目负责人。我方保证上述信息的真实和准确,如果发现并证实项目经理有在建工程,我方愿意自动放弃中标资格。
 特此承诺。
   投标人：中国移动通信集团河南有限公司
   法定代表人：赵超
   日期：2021年11月12日

承诺作出日期： 2021-11-12

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺类型：	证明事项型	第 46 条
承诺事由：	不拖欠农民工工资承诺书	
承诺作出日期：	2021-12-27	
承诺受理单位：	新乡市公共资源交易管理中心	
承诺履行状态：	——	

企业信用承诺信息

承诺类型：	证明事项型	第 47 条
承诺事由：	不拖欠农民工工资承诺书	
承诺作出日期：	2021-12-28	
承诺受理单位：	新乡市公共资源交易管理中心	
承诺履行状态：	——	

企业信用承诺信息

承诺类型：	主动型	第 48 条
承诺事由：	资料真实性承诺书	
承诺作出日期：	2021-12-28	
承诺受理单位：	新乡市公共资源交易管理中心	
承诺履行状态：	——	

企业信用承诺信息

承诺类型：	证明事项型	第 49 条
承诺事由：	项目经理无在建承诺书	
承诺作出日期：	2021-12-27	

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 证明事项型 第 50 条

承诺事由： 投标信誉承诺书

承诺作出日期： 2021-12-26

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺编码： 410700202111103G71383 第 51 条

承诺类型： 证明事项型

承诺事由： 投标信誉承诺书

承诺内容： <p style="text-indent:2em;"><table border="0" cellpadding="0" cellspacing="0" width="629" style="width:472pt;" class="ke-zeroborder"><tbody><tr><td height="187" class="xl65" width="629"> <h1 style="text-align:center;">信誉承诺书 </h1>延津县产业集聚区管理委员会:
   我方在此承诺，我方信誉良好，现阶段没有处于被责令停产、停业，或者投标资格被取消，无骗取中标或者严重违约或者重大工程质量安全生产事故等问题；我方承诺上述信息的真实和准确，一经发现失实我方愿意无条件自动放弃中标资格。
特此承诺
   投标人：中国移动通信集团河南有限公司
   法定代表人：张建国
   日期：2021-11-03</td></tr></tbody></table></p>

承诺作出日期： 2021-11-03

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代 124107006716746398

码：

企业信用承诺信息

承诺编码：41070020211103C[illegible]102　　第 52 条

承诺类型：行业自律型

承诺事由：全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺内容：<h2 style="text-align:center;">全省房屋建筑和市政基础设施工程项目招标投标活动承诺书</h2>   我单位承诺,在延津县产业集聚区管理委员会智慧化工园区信息平台（一期）建设工程项目项目招投标活动中,自觉遵守《中华人民共和国招标投标法》、《中华人民共和国招标投标法实施条例》、河南省实施《中华人民共和国招标投标法》办法等招标投标相关法律、法规和制度规定,如有违反,愿承担相关法律责任。
   投标人： 中国移动通信集团河南有限公司
   承诺人（法人代表）： 张建国
   日期： 2021年11月03日

承诺作出日期：2021-11-03

承诺履行状态：全部履行

承诺受理单位：新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码：124107006716746398

企业信用承诺信息

承诺编码：41070020211122H04434　　第 53 条

承诺类型：证明事项型

承诺事由：项目经理无在建承诺书

承诺内容：<h1 style="text-align:center;">项目经理无在建承诺书</h1>获嘉县卫生健康委员会:
<span style="font-family:FangSong_GB2312;font-

size:16px;">   我方在此声明,我方拟派往获嘉县医共体信息化平台服务项目二次(以下简称“本工程”)的项目经理在本项目报名之日起不再担任其他正在施工建设项目的项目经理或项目负责人。我方保证上述信息的真实和准确,如果发现并证实项目经理有在建工程,我方愿意自动放弃中标资格。
 特此承诺。
   投标人：中国移动通信集团河南有限公司
   法定代表人：赵超
   日期：2021年11月22日

承诺作出日期： 2021-11-22

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺编码： 41070020210907G18841 第 54 条

承诺类型： 主动型

承诺事由： 资料真实性承诺书

承诺内容： <h1 style="text-align:center;">资料真实性承诺书</h1>延津县应急管理局:
   我方在此声明,我方所提供的以上资料均真实和准确。我方保证上述信息的真实和准确,并愿意承担因我方就此弄虚作假所引起的一切法律后果。
特此承诺。
   投标人:中国移动通信集团河南有限公司
   法定代表人:杨威
   日期：2021-09-07

承诺作出日期： 2021-09-07

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代 124107006716746398

码：

企业信用承诺信息

承诺编码：4107002021110 3G37255　　第 55 条

承诺类型：主动型

承诺事由：资料真实性承诺书

承诺内容：<h1 style="text-align:center;">资料真实性承诺书</h1>延津县产业集聚区管理委员会:
   我方在此声明,我方所提供的以上资料均真实和准确。我方保证上述信息的真实和准确,并愿意承担因我方就此弄虚作假所引起的一切法律后果。
特此承诺。
   投标人:中国移动通信集团河南有限公司
   法定代表人:张建国
   日期：2021-11-03

承诺作出日期：2021-11-03

承诺履行状态：全部履行

承诺受理单位：新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码：124107006716746398

企业信用承诺信息

承诺编码：41140020170907003371　　第 56 条

承诺类型：主动型

承诺事由：自愿注册加入“商丘市公共资源交易服务平台市场主体库”

承诺内容：一、在市场主体库发布的相关信息均真实有效，我单位（个人）愿意接受行政、行业及社会监督。二、进行的所有操作均是我单位（个人）的真实意思表示并对其真实性、合法性负责，同意因保管不善所造成的一切不利后果由我单位（个人）自行承担。三、如

因出现对法律、法规及交易文件内容不知道、不清楚导致的误操作，不利后果由我单位（个人）自行承担。

承诺作出日期： 2017-09-07

承诺履行状态： 全部履行

承诺受理单位： 商丘市公共资源交易中心

承诺受理单位统一社会信用代码： 124[illegible]1400MB0W227[illegible]9B

企业信用承诺信息

承诺类型： 证明事项型　　第 57 条

承诺事由： 项目经理无在建承诺书

承诺作出日期： 2021-12-26

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 主动型　　第 58 条

承诺事由： 办理业务作出承诺

承诺作出日期： 2021-06-22

承诺受理单位： 郑州市信息中心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 证明事项型　　第 59 条

承诺事由： 不拖欠农民工工资承诺书

承诺作出日期： 2021-12-28

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息 第 60 条

承诺类型： 证明事项型

承诺事由： 投标[illegible]誉承诺书

承诺作出日期： 2021-12-[illegible]

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息 第 61 条

承诺类型： 证明事项型

承诺事由： 申报项目

承诺作出日期： 2022-03-17

承诺受理单位： 河南省发展和改革委员会

承诺履行状态： — —

企业信用承诺信息 第 62 条

承诺编码： 410700202111103G43255

承诺类型： 证明事项型

承诺事由： 不拖欠农民工工资承诺书

承诺内容： <h1 style="text-align:center;">不拖欠农民工工资承诺书</h1>延津县产业集聚区管理委员会:
   若我公司中标,我公司承诺在(项目名称)施工期间不拖欠农民工工资,建立支付农民工工资专项保证金。
   我公司保证不拖欠农民工工资,一定将农民工工资足额直接发放到农民工手中,并保证将每月工资发放表及时上报给贵公司,并保证资料的真

实有效性;如有虚假和不报的情况发生,我公司愿意接受贵单位的处罚。

   投标人：中国移动通信集团河南有限公司

   法定代表人：张建国

    日期：2021年11月03日

承诺作出日期： 2021-11-03

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 12410700671674639 8

企业信用承诺信息

承诺编码： 41010020220826025180 第 63 条

承诺类型： 主动型

承诺事由： 申报2022年郑州市制造业高质量发展专项资金

承诺内容： 所提交的申报材料内容和所附资料均合法、真实、有效，并对所提供资料的真实性负责。

承诺作出日期： 2022-08-26

承诺履行状态： 全部履行

承诺受理单位： 郑州市工业和信息化局

承诺受理单位统一社会信用代码： 11410100005253103F

企业信用承诺信息

承诺类型： 主动型 第 64 条

承诺事由： 资料真实性承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 65 条

承诺类型： 主动型

承诺事由： 资料真实性承诺书

承诺作出日期： 2021-12-28

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 66 条

承诺编码： 410700202111 22G62011

承诺类型： 证明事项型

承诺事由： 投标信誉承诺书

承诺内容： <p style="text-indent:2em;"><table border="0" cellpadding="0" cellspacing="0" width="629" style="width:472pt;" class="ke-zeroborder"><tbody><tr><td height="187" class="xl65" width="629"> <h1 style="text-align:center;">信誉承诺书</h1>获嘉县卫生健康委员会:
   我方在此承诺，我方信誉良好，现阶段没有处于被责令停产、停业，或者投标资格被取消，无骗取中标或者严重违约或者重大工程质量安全生产事故等问题；我方承诺上述信息的真实和准确，一经发现失实我方愿意无条件自动放弃中标资格。
特此承诺
   投标人：中国移动通信集团河南有限公司
   法定代表人：赵超
   日期：2021-11-22</td></tr></tbody></table></p>

承诺作出日期： 2021-11-22

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

第 67 条

承诺类型： 行业自律型

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 68 条

承诺类型： 证明事项型

承诺事由： 投标信誉承诺书

承诺作出日期： 2021-12-26

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

第 69 条

承诺编码： 410700202109 07G60844

承诺类型： 证明事项型

承诺事由： 项目经理无在建承诺书

承诺内容： <h1 style="text-align:center;">项目经理无在建承诺书</h1>延津县应急管理局:
   我方在此声明,我方拟派往延津县应急指挥平台硬件建设项目(以下简称“本工程”)的项目经理在本项目报名之日起不再担任其他正在施工建设项目的项目经理或项目负责人。我方保证上述信息的真实和准确,如果发现并证实项目经理有在建工程,我方愿意自动放弃中标资格。
 特此承诺。
   投标人：中国移动通信集团河南有限公司
   法定代表人：杨威
   日期：2021年09月07日

承诺作出日期： 2021-09-07

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 12410700671674639 8

企业信用承诺信息

承诺编码： 410700202111122G46481 第 70 条

承诺类型： 证明事项型

承诺事由： 不拖欠农民工工资承诺书

承诺内容： <h1 style="text-align:center;">不拖欠农民工工资承诺书</h1>获嘉县卫生健康委员会:
   若我公司中标,我公司承诺在(项目名称)施工期间不拖欠农民工工资,建立支付农民工工资专项保证金。
   我公司保证不拖欠农民工工资,一定将农民工工资足额直接发放到农民工手中,并保证将每月工资发放表及时上报给贵公司,并保证资料的真实有效性;如有虚假和不报的情况发生,我公司愿意接受贵单位的处罚。
   投标人：中国移动通信集团河南有限公司
   法定代表人：赵超
   日期：2021年11月22日

承诺作出日期： 2021-11-22

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺编码： 410700202111112G28920 第 71 条

承诺类型： 行业自律型

承诺事由： 全省房屋建筑和市政基础设施工程项目招标投标活动承诺书

承诺内容： <h2 style="text-align:center;">全省房屋建筑和市政基础设施工程项目招标投标活动承诺书</h2>   我单位承诺,在获嘉县医共体信息化平台服务项目项目招投标活动中,自觉遵守《中华人民共和国招标投标法》、《中华人民共和国招标投标法实施条例》、河南省实施《中华人民共和国招标投标法》办法等招标投标相关法律、法规和制度规定,如有违反,愿承担相关法律责任。
   投标人：中国移动通信集团河南有限公司
   承诺人（法人代表）：赵超
   日期：2021年11月12日

承诺作出日期： 2021-11-12

承诺履行状态： 全部履行

承诺受理单位： 新乡市公共资源交易管理中心

承诺受理单位统一社会信用代码： 124107006716746398

企业信用承诺信息

承诺类型： 证明事项型　　第 72 条

承诺事由： 项目经理无在建承诺书

承诺作出日期： 2021-12-27

承诺受理单位： 新乡市公共资源交易管理中心

承诺履行状态： — —

企业信用承诺信息

承诺类型： 证明事项型　　第 73 条

承诺事由： 项目备案信息承诺

承诺作出日期： 2021-12-21

承诺受理单位： 新乡经济技术开发区管理委员会

承诺履行状态： — —

七、信用评价信息 (共 0 条)

此项信息相关部门暂未提供

八、司法判决及执行信息 (共 0 条)

此项信息相关部门暂未提供

九、其他信息 (共 0 条)

查询期内无相关记录

十、信用状况提升建议

建议秉持诚信理念，合法有序开展经营活动。

结束

公共资源交易平台技术规范

十一、投标人诚信承诺书

诚 信 承 诺 书

为维护市场公平竞争，营造诚实守信的公共资源交易环境，本公司郑重承诺：

1、本次投标在电子投标文件中的所有信息均真实有效，提交的材料无任何伪造、修改或虚假成份，材料所述内容均为本公司真实拥有。若违反本承诺，一经查实，本公司愿意接受公开通报，自愿退出所有正在进行的交易项目，按照《中华人民共和国政府采购法》第七十七条和《中华人民共和国政府采购法实施条例》等相关法律规定，主动接受处罚，并承担相应法律责任；

2、本公司在参加本项目过程中严格遵守各项诚信廉洁规定，如有违反，自愿按规定接受处罚。

承诺人法定名称（盖章）：中国移动通信集团河南有限公司

承诺人法定地址：郑州市经三路 48 号

授权代表（签字或盖章）：

电话：18211872137

2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C19CE6776467E1A6...

一、投标书

投　标　书

致：南阳市政府采购中心

根据贵方招标编号为（ 南阳政采公开-2023-111 ） 的投标邀请，签字代表 张航、解决方案经理 （全名、职务）经正式授权并代表投标人 中国移动通信集团河南有限公司、郑州市经三路 48 号（投标人名称、地址）提交电子投标文件一份，并对之负法律责任。

投标文件组成：开标一览表及资格证明文件第 1 至 11 项，商务及技术文件第 1 至 9 项。

据此函，签字代表宣布同意如下：

1、所附投标分项报价一览表中提供的报价为以开标一览表为准。

2、如果我们的投标书被接受，我们将履行招标文件中规定的每一项要求，按期、按质、按量履行合同。

3、我方愿按《中华人民共和国政府采购法》和《中华人民共和国民法典》履行我方的全部责任。

4、我方已详细审查全部招标文件，包括修改文件以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明白及误解的权力。

5、本投标自开标之日起有效期为 60 天。

地址：郑州市经三路 48 号　　电话（传真）：0371-68588012

法定代表人（负责人）或授权代表（签字）：

投标人名称（公章）：中国移动通信集团河南有限公司

日期：　2023　年　12　月　22　日

公共资源交易平台投标专用

二、分项报价一览表

服务项部分：

类型	序号	名称	说明	规格	计费规则	服务最高限价（元/月）	投标报价
计算	1	云主机 VCPU		1 核	根据规格及数量按月计费，由弹性伸缩增加的实例按月计费	40	40
	2	云主机内存		1G		12	12
	3	云主机（GPU 基础版）	提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不 低于 128bits。（直通型）	8 核 32G	根据规格及数量按月计费，由弹性伸缩增加的实例按月计费	1301	1300
	4		提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不 低于 128bits。（虚拟化）	8 核 32G		868	850
	5	云主机（GPU 标准版）	提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*2 GDDR6 显存、位宽 不低于 128bits。（直通型）	16 核 64G		2603	2580
	6		提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*2 GDDR6 显存、位宽 不低于 128bits。（虚拟化）	16 核 64G		1736	1710
	7		提供 V100 卡或同档显卡，提 供高性能图形计算加速，提供 不低于 32G*1 显存、位宽不低于 256bits。（直通型）	16 核 64G		2399	2380

公共资源交易平台技术专用

	8		提供 V100 卡或同档显卡，提 供高性能图形计算加速，提供 不低于 32G*1 显存、位宽不低于 256bits。（虚拟化）	16 核 64G		1634	1610
	9	云主机（GPU 高级版）	提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*4 GDDR6 显存、位宽不低于 128bits。（直通型）	32 核 128G		5205	5180
	10		提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*4 GDDR6 显存、位宽不低于 128bits。（虚拟化）	32 核 128G		3470	3450
	11		提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G*2 显存、位宽不 低于 256bits。（直通型）	32 核 128G		4798	4770
	12		提供 V100 卡或同档显卡，提 供高性能图形计算加速，提供 不低于 32G*2 显存、位宽不低于 256bits。（虚拟化）	32 核 128G		3266	3250
	13	物理机（计算型）	2 路	单 CPU>=10 核，Mem>=64G,本地硬盘(SAS 盘)>=600G*2	根据规格及数量按月计费，由弹性伸缩增加的实例按月计费	658	640
	14			单 CPU>=10 核，Mem>=128G,本地硬盘(SAS 盘)>=600G*2		708	690
	15			单 CPU>=10 核，Mem>=192G,本地硬盘(SAS 盘)>=600G*2		759	750

公共资源交易平台技标专用
AE2C19CEC7764E1A62A8BC88EA14DB9

	16			单 CPU>=10 核，Mem>=256G，本地硬盘(SAS 盘)>=600G*2		809	790
	17			单 CPU>=10 核，Mem>=384G，本地硬盘(SAS 盘)>=600G*2		1012	990
	18			单 CPU>=10 核，Mem>=512G，本地硬盘(SAS 盘)>=600G*2		1214	1200
	19			单 CPU>=10 核，Mem>=128G，本地硬盘(SAS 盘)>=600G*2		1460	1450
	20		4 路	单 CPU>=10 核，Mem>=192G，本地硬盘(SAS 盘)>=600G*2		1511	1490
	21			单 CPU>=10 核，Mem>=256G，本地硬盘(SAS 盘)>=600G*2		1561	1540
	22			单 CPU>=10 核，Mem>=512G，本地硬盘(SAS 盘)>=600G*2		2060	2050

中国移动通信集团河南有限公司
公共资源交易平台招标专用
AE2C19CEC77646E1162B8BC88EA14DB9

	23	GPU 卡	物理机叠加，单卡提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16GGDDR6 显存、显存位宽不低于 256bits。	块		572	550
	24		物理机叠加，单卡提供 V100 卡或同档显卡，提供高性能图 形计算加速，提供不低于 32G 显存，位宽不低于 256bits。	块		1011	1000
操作系统	25	Linux Server	根据需要提供合适的版本（包括国产操作系统）	实例		21	20
	26	Windows Server	根据需要提供合适的版本	实例		41	41
存储	27	低 IO	适用于云硬盘、文件存储、对象存储，介质为 SATA,HDD，30MB/s<吞吐量<40MB/s，100<IOPS<1000。	TB	根据快照所占的存储空间大小按月计费	93	93
	28	中 IO	适用于云硬盘，介质为 SAS 盘 HDD，40MB/s<吞吐量 140MB/s，1000<IOPS<5000	TB		119	119
	29	高 IO	适用于云硬盘，介质为 SSD 盘，140MB/s< 吞吐量 <300MB/s ，5000<IOPS<25000	TB		324	324
	30	视频存储		TB		26	25
	31	共享存储	适用于共享云硬盘，具备多挂 载点、高并发性、高性能、高 可靠性等特点。主要应用于需要支持集群、HA（High Available，指高可用集群）能力的关键企业应用场景，多个云服务器可同时访问一个共享云硬盘，FC-SAN 存储空间，介质为 SAS 盘 HDD	TB		397	395
数据备份	32	虚拟机/文件备份	本地备份	TB		101	101
	33		异地备份（定时）	TB		112	112
	34		异地备份（实时）	TB		121	121
	35	数据库备份	本地备份	TB		101	101
	36		异地备份（定时）	TB		112	112
	37		异地备份（实时）	TB		121	121

公共资源交易平台技标专用
AE2C19C8777646E1A62A8BC88EA14DB9

负载均衡	38	虚拟负载均衡			实例	11	10
云数据库	39	关系型数据库	提供稳定可靠、可弹性伸缩的 在线数据库服务，是一种高安 全、高可用，易运维的 MySQL 数据库，提供备份、恢复、监 控服务等基本功能，配合提供数据库基础运维服务，需搭配 块存储使用，存储另行计费。	2 核 4G，最大连接 数：1200	计费方式：根据实例个数+规格 按月计费	59	55
	40			4 核 8G，最大连接 数：2000		119	115
	41			8 核 16G，最大连接数： 4000		236	230
	42			16 核 64G，最大连接数： 16000		513	500
	43			32 核 128G，最大连 接数：20000		1026	990
	44		关系型数据库 Oracle，提供安装与激活服务，提供数据库 基础运维服务。	数据库实例	计费方式：根据实例个数+规格 按月计费	700	600
	45		SQL Server 拥有高可用架构和数据恢复功能，包含 License 授权，支持实例管理、账号管理、数据库管理、白名单、备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存 储另行计费。	2 核 4G	根据实例规格和个数+存储空间按月计费	248	240
	46			2 核 8G		251	240
	47			4 核 16G		502	490
	48			8 核 16G		990	980
	49			8 核 32G		1003	990
	50			16 核 32G		1980	1700
	51		缓存数据库 Redis，提供数据 监控、数据管理、数据安全、 备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存储另行计费。集群版： 主从版*2	主从版-2G	根据实例规格和个数+存储空间按月计费	44	44
	52			主从版-4G		87	85
	53			主从版-8G		174	170
	54			主从版-16G		348	340
	55			主从版-32G		696	690
	56			主从版-64G		1392	1200
	57			集群版-16G		696	690
	58			集群版-32G		1392	1200
	59			集群版-64GB		2783	2500

公共资源交易平台技标专用

	60		关系型数据库 PostgreSQL，配合提供数据库基础运维服	2 核 4G，最大连接数 1200，最大 IOPS 2500	根据实例规格和个数+存储空间按月计费	59	57
	61			2 核 8G，最大连接数 1600，最大 IOPS 3500		83	80
	62			2 核 16G，最大连接数 2500，最大 IOPS 4500		107	105
	63			4 核 16G，最大连接数 4000，最大 IOPS 7000		165	160
	64			4 核 32G，最大连接数 5000，最大 IOPS 9000		212	210
	65			8 核 64G，最大连接数 10000，最大 IOPS 18000。		425	420
	66			16 核 128G，最大连接数 12000，最大 IOPS 36000		851	840
	67	分布式关系型数据库	基于普通服务器和横向扩展 的方式，构建支持海量数据存 储和访问的数据库系统，从而实现无线扩容和弹性扩展。	2 核 8G，最大连接数 1600，最大 IOPS 3500	根据实例规格和个数+存储空间按月计费	83	80
	68			2 核 16G，最大连接数 2500，最大 IOPS 4500		107	105
	69			4 核 16G，最大连接数 4000，最大 IOPS 7000		165	160

公共资源交易平台技术专用
AE2C19CEC77646E1A6C1BC88EA14DB9

	70			4 核 32G，最大连接数 5000，最大 IOPS 9000		212	210
	71			8 核 64G，最大连接数 10000，最大 IOPS 18000。		425	420
	72			16 核 128G，最大连接数 12000，最大 IOPS 36000		851	800
	73	分布式文档数据库	基于分布式文档数据库，提供 稳定可靠、可弹性伸缩的在线 数据库服务，是一种高安全、 高可用，易运维的数据库，提 供备份、恢复、监控服务等基 本功能，配合提供数据库基础运维服务。	2 核 8G	根据实例规格和个数+存储空间按月计费	194	190
	74			4 核 16G		389	380
	75			8 核 32G		777	765
	76			16 核 64G		1553	1400
	77	国产数据库	提供不少于三种国产数据库，提供租用、安装、调优、排错、技术支持。	1CPU	根据实例开通的 CPU 数按月计费	432	425
大数据服务	78	实时计算	提供流式计算引擎，将各种不同的数据源中的数据进行实 时的订阅、处理、分析。	1CPU+4G 内存		86	80
	79	离线计算	服务于批量结构化数据的存 储和计算，可以提供海量数据 仓库的解决方案，存储另算。	1CPU+4G 内存		71	70
	80	搜索引擎	提供数据分析、搜索等场景服 务，存储另算。	1CPU+4G 内存		78	75
	81	分析计算	提供对海量数据进行即时的 多维分析透视和业务探索，快速构建数据仓库，存储另算。	1CPU+4G 内存		94	90
容器服务	82	容器服务	根据部署容器的节点数按月计费（仅包括节点管理费用，不包含资源费用，云服务器/云服务器_Disk/负载		根据部署容器的节点数按月计费	166	160

中国移动通信集团河南有限公司
公共资源交易平台专用

			均衡/EIP/专有网络等资源另行计算）				
应用服务	83	应用与数据集成服务	提供将物联网、大数据、视频、统一通信、GIS 等基础平台及各个应用的服务、消息、数据统一集成适配以及编排的能力。		链接/月	210	200
	84	应用管理	应用管理平台，提供资源及业务应用的实时监控、实时告警事件、统一日志收集和分析等功能。		VCPU/月	819	750
	85	应用工厂服务	应用管理与运维平台为开发人员、测试人员、运维人员或项目经理等角色，提供应用托管、监控、告警和日志分析等能力提供以应用为中心的应用发布、部署、监控、告警、日志等一站式管理能力。	1VCPU/月	根据服务核数按月计费	328	320
	86	应用迁移	系统迁移服务	1 虚机/次	按次计费	3000	2500
网络及托管服务	87	互联网带宽	提供互联网访问独享带宽 2-100Mbps 部分，每 2 兆带宽 40 元，超过 100M 部分，每 2 兆带宽 34 元）	2Mbps	根据实例开通的带宽数量按月计费	40	40
	88	互联网 IP	提供互联网 IP 地址，IPv4 版（IPv6 地址免费）	1 个	根据实例开通的 IP 数量按月计费	100	100
	89	设备托管	提供 1U 托管机位	1U	根据实际占用数量按月计费	200	200
	90		提供 42U 标准托管机架（3.5KW）	1 架	根据实际占用数量按月计费	4000	4000
云桌面	91	云桌面	提供云桌面授权，不含终端，支持软拨号。	用户/月	根据实际开通数量按月计费	200	200
合计：						74088	71608
优惠率：						3.35%	

公共资源交易平台投标专用

云租户安全部分：

类别	名称	技术指标	服务最高限价	投标报价
云安全	虚拟防火墙	提供虚拟网络安全区域边界安全防护能力。	180 万/年	177 万/年
	虚拟漏洞扫描	提供虚拟化漏洞扫描功能，包含数据库漏洞扫描、系统漏洞扫描、WEB 漏洞扫描、主机基线配置核查、网络基线配置核查等功能模块，提供报告。		
	虚拟堡垒机	提供虚拟化运维安全管理、审计系统(堡垒机)安全能力		
	虚拟主机安全	虚拟机形态部署，提供资产管理、安全体检、安全监控、漏洞风险、入侵威胁、合规基线等多个功能模块，各个模块进行联动，模块间数据联通，形成闭环系统，为企业提供强有力的采集、检测、监测、防御、捕获能力，对主机进行全方位的安全防护。		
	虚拟 Web 应用防火墙	提供虚拟化 WAF 安全能力。		
	网页防篡改	提供网页防篡改功能。		
	虚拟日志审计	提供日志分析系统，支持日志的采集、过滤、归并、关联分析、展现、告警监控、实施事件监控、报表等。		
	虚拟 VPN 安全接入	提供国密 SSLVPN 加密服务，移动办公安全接入，包括接入用户身份认证、传输数据加密、权限划分和接入审计，每 100 个 VPN 并发组件。		
	虚拟防病毒	提供虚拟化防病毒能力。		
	入侵检测	整机吞吐量≧10Gbps。		
	虚拟数据库审计	针对用户对数据库的访问行为进行记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源。加强内外部数据库网络行为记录，提高数据资产安全。		
	虚拟密码机	能够为政务云提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，可以满足通用密码服务，保证传输信息的机密性、完整性和有效性，司时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。		
	数据库加密服务	200 实例。		
优惠率：			1.67%	

公共资源交易平台投标专用

新增安全服务

序号	名称	技术参数	投标报价
1	云资源监控	支持对云平台的各类云资源进行监控，提取各类云资源的监控指标，并支持设定阈值产生相应的阈值告警；	0 元
2	数据安全服务 DSC	提供数据分级分类、敏感数据识别、数据水印溯源和数据静态脱敏等基础数据安全能力，通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势；	
3	密钥管理服务 KMS	为平台云服务、租户业务应用提供一种安全可靠、简单易用的密钥托管服务	
4	凭据管理服务 CSMS	通过凭据管理服务，创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期和统一管理	
5	安全指数服务 SIS	通过安全指数服务了解所使用云环境是否已合理配置，所采取的安全措施是否已经足够，以及主动安全、被动安全的概况	
6	安全云脑 SecMaster	提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力	
7	安全组	通过配置安全规则来控制云主机网络消息的流入流出，只允许授权的消息通过	
8	网络 ACL	通过与子网关联的出方向/入方向规则控制出入子网的数据流	
9	AntiDDoS	通过对互联网访问公网 IP 的业务流量进行实时监测，及时发现异常 DDoS 攻击流量。	
10	网闸	通过在网络模型的各层的断开，阻断了对内网具有潜在攻击可能的一切网络连接，使外部攻击者无法直接入侵、攻击或破坏内网，保障了内部主机的安全	

公共资源交易平台竞标专用

三、项目技术方案、应急保障服务能力方案、承诺书等

3.1 政务云需求现状分析

3.1.1 项目背景

近年来，随着信息技术的快速发展和革新，加强数字政府建设是适应新一轮科技革命和产业变革趋势，加快数字化发展是建设网络强国、数字中国的基础性工程。南阳市政府以《“十四五”推进国家政务信息化规划》、《国务院关于加强数字政府建设的指导意见》、《全国一体化政务大数据体系建设指南》要求以及河南省、南阳市相关政策为导向，统筹建设全市统一的政务信息化基础设施，进一步降低行政成本，提高行政效率，为我市推动数字政府建设，助力政府数字化转型和智慧城市建设打下坚实基础。

3.1.1.1 国家政策

2021 年，国家发展改革委印发《“十四五”推进国家政务信息化规划》，要求完善国家电子政务网络，集约建设政务云平台和数据中心体系，综合运用新技术新理念新模式提升治理能力、优化公共服务。主要任务在三个方面：一是发展壮大融合创新大平台。加快网络融合，升级完善国家电子政务网络体系，加快技术融合，构建智能化政务云平台体系，加快数据融合，健全国家数据共享与开放体系，加快服务融合，完善全国一体化政务服务平台体系。二是深度开发利用政务大数据。深化基础信息库共享应用，建设经济治理基础数据库。三是统筹建设协同治理大系统。提升执政能力信息化水平，强化依法治国信息化基础，优化经济治理信息化协同，完善市场监管信息化支撑，加强公共安全信息化保障，健全环境保护信息化能力。

2022 年，国务院发布《国务院关于加强数字政府建设的指导意见》和《全国一体化政务大数据体系建设指南》强化安全可信的信息技术应用创新，充分利用现有政务信息平台，整合构建结构合理、智能集约的平台支撑体系，适度超前布局相关新型基础设施，全面夯实数字政府建设根基。

（一）强化政务云平台支撑能力。

公共资源交易平台投标专用

依托全国一体化政务大数据体系，统筹整合现有政务云资源，构建全国一体化政务云平台体系，实现政务云资源统筹建设、互联互通、集约共享。国务院各部门政务云纳入全国一体化政务云平台体系统筹管理。各地区按照省级统筹原则开展政务云建设，集约提供政务云服务。探索建立政务云资源统一调度机制，加强一体化政务云平台资源管理和调度。

（二）提升网络平台支撑能力。

强化电子政务网络统筹建设管理，促进高效共建共享，降低建设运维成本。推动骨干网扩容升级，扩大互联网出口带宽，提升网络支撑能力。提高电子政务外网移动接入能力，强化电子政务外网服务功能，并不断向乡镇基层延伸，在安全可控的前提下按需向企事业单位拓展。统筹建立安全高效的跨网数据传输机制，有序推进非涉密业务专网向电子政务外网整合迁移，各地区各部门原则上不再新建业务专网。

（三）加强重点共性应用支撑能力。

推进数字化共性应用集约建设。依托身份认证国家基础设施、国家人口基础信息库、国家法人单位信息资源库等认证资源，加快完善线上线下一体化统一身份认证体系。持续完善电子证照共享服务体系，推动电子证照扩大应用领域和全国互通互认。完善电子印章制发、管理和使用规范，健全全国统一的电子印章服务体系。深化电子文件资源开发利用，建设数字档案资源体系，提升电子文件（档案）管理和应用水平。发挥全国统一的财政电子票据政务服务平台作用，实现全国财政电子票据一站式查验，推动财政电子票据跨省报销。开展各级非税收入收缴相关平台建设，推动非税收入收缴电子化全覆盖。完善信用信息公共服务平台功能，提升信息查询和智能分析能力。推进地理信息协同共享，提升公共服务能力，更好发挥地理信息的基础性支撑作用。

3.1.1.2 **河南省政策**

2023 年，河南省人民政府印发《河南省加强数字政府建设实施方案（2023—2025 年）》，总体要求坚持集约化、规模化、绿色化方向，着力优化结构布局，强化省市统筹，推动整合共建，实施全栈集成，提升服务效能，构建逻辑集中、互联互通、先进智能、安全可靠的全省一体化政务云体系，全量高效承载各类非涉密政务信息系统，全面实现政务数据汇聚治理和业务应用整体协同，为全面建设

公共资源交易平台投标专用

高水平数字政府提供功能强大的云支撑。

3.1.1.3 南阳市政策

2022 年，市政府常务会议研究通过了《南阳市数字政府建设实施方案(2022-2025)》宛政办〔2022〕50 号提出完善市政务云平台，按照全省政务云平台“1+18”的布局，通过政务外网实现与全省政务云平台其他节点间的互联。通过购买服务方式选择优质政务云供应商，以“按需分配、弹性服务”的原则为市、县（区）各部门提供统一的云计算、云存储、云管控、云安全等云服务。逐步实现各个部门系统的上云迁移、数据资源汇聚共享、业务应用高效协同，为数字政府建设提供集约化基础支撑。

优化云资源管控和服务。搭建政务云资源运营管控平台，统一管理和调度计算、存储、网络等资源，实现对资源的实时监控、综合分析、快速部署、动态扩展，提高云资源的管理、服务和承载能力。出台全市政务云建设和使用管理办法，明确政务云平台建设、资源申请、集中调度和综合服务运行机制。

3.1.2 项目现状

3.1.2.1 现网建设总述

原南阳市政务云是 2017 年南阳市政府第 50 次常务会研究决定建设的“三基础两重点”项目之一，采用了“运营商建设运维，政府采购服务”的建设模式，由南阳移动承建，截止目前，已平稳运行 6 年，实现安全“0”事故，运行期间荣获中国数据中心产业发展联盟“2017-2018 年度数据中心推荐产品/解决方案”奖。

原政务云平台基于华为 HCS（Huawei Cloud Stack 6.5.1.SPC10）技术架构搭建。计算层按 OpenStack Nova AZ 接入不同的资源池，划分为政务公有云区资源池和政务专有云区资源池，两区之间通过网闸进行物理隔离，实现数据摆渡；存储层虚拟资源池使用 IPSAN 存储和 FusionStorage 分布式存储；云服务层采用统一的云服务 Console，接入 ManageOne 实现云平台管理。目前主要向租户提供 ECS、EVS、IMS、VPC、SG、EIP、VFW、AS、CSBS、RDS、BMS 等云服务。

政务公有云：面向市级政府部门提供电子政务外网互联网业务区云服务，承载各市级政府部门有互联网访问需求的门户网站、互联网服务大厅等面向公众的业务。双核心交换机（ZTE9908）向下连接区内管理和控制服务器，该区内计

公共资源交易平台技标云用

算节点和存储服务器通过业务接入交换机和存储接入交换机连接到核心交换机上；核心交换机物理旁挂、逻辑上串联防病毒网关、业务防火墙（E8000E-X8）和负载均衡设备；出口采用 20G 光纤与运营商互联网相连，并部署有 DDoS 检测和清洗、入侵防御等安全设备。

政务专有云：面向市级政府部门提供电子政务外网公共业务区云服务，承载各厅局内部业务系统、数据库系统等业务；出口使用双 10G 光纤与市电子政务外网相连，双核心交换机（ZTE9908）向下连接区内管理和控制服务器，并部署有入侵防御、防病毒网关、核心防火墙等安全设备。

原政务云平台为南阳市“互联网+政务服务”建设奠定了坚实的平台基础，在河南省创造了五个“第一”，即：第一个按照云服务模式建设的政务云；第一个由运营商提供一栋专用 IDC 机房楼部署政务云的项目；第一个实现政务专有云和公有云分别与电子政务外网和互联网相通，并实现数据有效共享的政务云；第一个建设了 PaaS 平台，为政务大数据融合共享奠定了基础；第一个由基础电信运营商专门成立专业运维团队的政务云运维中心。

3.1.2.2 现网资源情况分析

原政务云先后历经 4 次扩容，截至目前云平台共使用机架 86 架，高性能服务器 207 台、网络设备 117 台和安全设备 43 台，可以对外提供 2.6 万核 VCPU、70.16TB 内存的服务能力。

原政务云平台共有 14 套存储，累计提供存储能力资源为 7.1PB。其中电子政务外网 4 套集中式存储，1 套分布式块存储共 36 台节点，1 套分布式文件存储共 8 台节点，1 套对象存储。互联网业务区部署 3 套集中式存储、1 套分布式块存储共 20 个节点、1 套文件存储共 8 个节点。

运行 6 年累计上云单位市直 46 家、县区 42 家，上云业务系统 151 个，累计发放服务器 1164 台。目前承载了南阳市政务服务平台、全面健康卡、基层 HIS、12345 市民服务热线、“宛快办”等重要基础信息平台，涉及政务、医疗、教育、民生等领域。

3.1.2.3 现网网络情况分析

政务云平台划分为政务公有云区和政务专有云区。政务公有云：面向市级政府部门提供电子政务外网互联网业务区云服务，承载各市级政府部门有互联网

访问需求的门户网站、互联网服务大厅等面向公众的业务，出口与运营商互联网相连。政务专有云：面向市级政府部门提供电子政务外网公共业务区云服务，承载各厅局内部业务系统、数据库系统等业务，出口与市电子政务外网相连。政务专有云与政务公有云之间采用跨域交换系统/网闸进行数据摆渡。

原政务云自下而上分为接入层、核心层、出口层三层，各层部署以下设备：

1、接入层：部署 TOR 和各类计算型服务器、存储设备。

2、核心层：部署业务、管理、存储、IPS、WAF 设备，负载均衡、防病毒网关等，旁挂核心防火墙，核心交换机向下汇聚交换网络内的所有接入层交换设备；业务、存储、管理独立部署；

3、出口层：出口层作为南阳移动政务云站点公有云区、专有云区的出口，通过出口层设备到达政务外网或互联网，实现与政务外网或互联网的互通；在互联网区出口旁挂抗 DDOS 设备，实现对来自互联网异常流量的引流、清洗、回注，实现对互联网区设备的按安全防护。

3.1.2.4 现网安全情况分析

南阳移动政务云专有云区通过核心交换机 ZTE9908 至信息中心出口来实现电子政务外网的互访，主要部署以下安全设备来对专有云区业务进行检测和防护。

1. 部署入侵检测设备针对应用流量做深度分析与检测。
2. 核心交换机与防火墙之间部署防病毒网关，防止病毒在网络传播扩散。
3. 防火墙旁路部署部署，开启虚墙功能，对各个局委进行隔离并进行严格的访问控制。
4. 核心交换机旁挂部署应用负载均衡设备，保证关键业务带宽，提升关键业务的高可用性。

南阳移动政务云互联网区通过 IDC NE40E 出口来实现互联网的互访，主要部署以下安全设备来对公有云区业务进行检测和防护。

1. 在网络出口旁路部署DDOS设备，对流量进行清洗。
2. 部署入侵检测设备针对应用流量做深度分析与检测。
3. 核心交换机与防火墙之间部署防病毒网关，防止病毒在网络传播扩散。

公共资源交易平台技术专用

4. 防火墙旁路部署部署，开启虚墙功能，对各个居委进行隔离并进行严格的访问控制。
5. 核心交换机旁挂部署应用负载均衡设备，保证关键业务带宽，提升关键业务的高可用性。
6. 在互联网核心区核心交换机旁路部署WAF（Web应用防火墙），保护Web应用通信流和所有相关的应用资源免受利用Web协议发动的攻击，并提供防病毒功能。

3.1.2.5 **现网运维情况分析**

河南移动南阳分公司综合部、政企部、网络部等部门组成横向管理团队，对南阳市政务云平台的市场和管理工作负责，其中政企部主要负责客户关系维护和合同签订等工作、综合部主要负责机房建筑的安全保卫与应急等、网络部传输动力中心主要负责动力环境管理和监控、网络部客户响应中心的政企支撑班主要负责平台运维和安全管理等工作。目前共有河南移动南阳分公司近 20 人参与云平台的运维工作。

原政务云平台涉及的公有云与专有云运营维护，配备专业的维护团队，提供全面的保障及运维服务，运维管理对象包括：机房、网络设备、安全设备、虚拟机、物理机、存储。集中专家资源解决运营维护过程中的各种疑难故障和问题，提升故障响应速度和本地业务支撑力度，确保南阳政务云平台高效、稳定、持续提供高可靠性的云服务。

1）为最终用户提供技术服务热线(7*24 小时)， 负责解答用户在云服务使用中遇到的问题，并及时提出解决问题的建议和操作方法。

2）在服务期内，提供 7*24 小时的现场和技术支持服务，对故障在半小时内响应，一般故障两小时内解决，较大故障根据实际情况原则上不超过 24 小时解决问题。

3）在服务期内，7*24 小时运行值班监控，配备具备多年云平台维护经验的运维人员，提供应急抢修支持。

基础设施及现场机房环境维护

对机房现场提供 7*24 小时驻场运维，机房所提供的基础设施维护内容包括：对政务云机房专有的配电系统、空调系统、消防系统、漏水检测系统及安防系统

的日常巡检及保养维护。同时通过 6 年的运维服务建立了一整套有效监控管理机制，运行 6 年机房安全“0”事故，并在疫情、建党 100 周年等关键时刻发挥了重要作用。

供配电系统维护

机房维护人员负责政务云机房所配备的冗余变压器、高压及低压配电系统、后备柴油发电机、UPS、开关电源等设备的日常巡检与维护，定期巡检、记录机房配电系统的运行情况，发现问题及时处理。

3.1.2.6 **现网问题汇总**

目前在用的南阳市政务云平台虽然取得一些成效，但随着云计算技术的持续发展，信息化产业需求不断升级，数据安全性凸显。平台当前面临的问题如下：

原政务云提供 IASS 层能力，满足计算、存储、网络、安全、备份等基础服务；具备基础的 PASS 能力。

安全方面：原政务云满足政务云等保三级要求，为满足国产信创要求，需增加数据库加密服务、虚拟密码机等能力。

国产化方面：原政务云当前基于 X86 服务器，操作系基于 Windows Server 和 Linux Server，为满足国产信创要求，需增加国产化操作系统（如麒麟、统信等），国产化数据库（如达梦、人大金仓等）。

PASS 高阶服务：原政务云平台 PASS 层高阶服务不足，为满足实际委办局业务需求，需增加云桌面服务、容器服务等。

多云纳管：按照省一朵云的规划及建设要求，原政务云平台不具备纳管能力，需增加多云纳管及一云多芯等能力。

弹性伸缩：目前现网政务云不能根据业务资源使用情况实现计算存储资源弹性扩展，出现资源利用率过低或过高情况。

综上所述，为满足平台的业务发展及安全需求，需要根据各单位业务需求引进政务云平台高阶服务（如：容器服务、应用服务、云桌面服务等）、国产化操作系统（如：麒麟、统信等）及国产化数据库（如：达梦、人大金仓等）、机房扩展服务（如：网络及托管服务等）及兼顾数据安全（如：数据库加密服务、虚拟密码机）。

3.1.3 需求分析

3.1.3.1 整体需求分析

根据南阳市政府关于政务云平台建设的相关要求，政务云主要为全市各政务部门提供云主机、裸金属、云存储、云应用、云安全和异地备份等基础设施资源共享服务，为各政务部门间数据交换、共享、应用等提供基础平台支撑。本项目服务对象是党政机关、事业单位等。

通过南阳市政务云服务能力建设，构建资源整合、管运分离、数据融合、业务贯通的数字政府市级政务云，为全市各级政府部门政务信息化系统建设提供一站式的机房环境、网络资源、存储资源、计算资源等云服务，实现市本级政务云的统一规划、统一管理，将市级政府部门从繁杂的信息化基础设施建设工作中解脱出来，将主要精力用在业务流程梳理和提高数字政府应用成效上。

南阳市政务云平台需要支持根据业务应用的不同特点分配不同的计算资源，包括采用合理的物理服务器。能根据业务应用的特点对服务器或存储进行配置满足应用对计算和存储的需要（CPU、内存、网络 I/O、存储 I/O,GPU）。从资源属性看，政务云平台的计算资源池划分为高性能计算区、GPU 计算区，通用性能计算区，物理机计算区，每个区分别使用不同的服务器进行承载。从资源池业务规划上看，政务云平台分为互联网区和政务外网区。计算平台需要和管理平台联动实现对虚拟计算资源的部署和分配。

存储与备份产品技术需求包含云存储服务、虚拟机/文件备份与异地灾备服务与数据库备份与异地灾备服务。云存储服务提供弹性扩展的虚拟块存储服务。像使用传统服务器硬盘一样，用户可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据做持久化存储。考虑到政务应用对存储性能要求不同，提供 SATA、SAS、SSD 等不同类型硬盘；虚拟机/文件备份与异地灾备服务是政务云平台需要实现本地备份的基础上同时考虑后续和容灾中心的联动，同时本地建设备份系统；数据库备份与异地灾备服务分两部分，一是云服务器备份服务，它为弹性云服务器提供整机及云硬盘备份功能，需要支持本地备份以及对备份数据的远程复制，并支持利用备份数据恢复云服务器数据，最大限度保障用户数据的安全性和正确性，确保业务安全，二是文件和数据库备份服务，它为租户提供快速、按需的企业级备份，需要帮助租户在云端构建备份系统。在发生灾难

公共资源交易平台招标专用

时可以自动或手动从云端快速恢复已备份的数据，避免在灾难发生时重要数据丢失对业务造成的影响，保证租户业务系统数据的可靠性及可用性。

政务云平台核心业务要求7*24小时不间断运行，一旦系统中断或无法运行，将会造成恶劣的社会影响。因此，为确保核心应用系统可靠稳定运行，云平台须具有高可靠性。应按照双路冗余方式进行网络整体设计和设备配置，消除单点故障，除带外管理网络外，所有网络应至少双链路接入，核心和重要设备需采用堆叠或其他技术手段实现设备间冗余，设备本身需满足双主控+多业务板卡冗余。同时考虑到政务业务多租户的特点，网络需支持多级VDC，虚拟私有云，云专线等网络服务，组网方式采用业界成熟和先进的SDN+VxLan组网。

云平台安全体系建设需要参考等级保护三级 2.0 基本要求进行设计，需要包含安全网络通信、安全区域边界、安全计算环境、安全管理中心。

租户侧需要考虑主机系统、应用系统安全风险，具备发现漏洞和资产核查能力，需要具备恶意代码防范能力，对外提供的 web 服务能力需要具备检测和防御 web 攻击的能力。需要具备云主机远程安全运维管理能力，日志审计能力，数据库审计能力等。

密码应用使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。基于密码算法风险，在本项目中要求按照相关政策要求，采用国家密码管理局批准的密码算法SM1/SM2/SM3/SM4。同时，要求所有硬件产品必须具有国家密码管理局的相关产品资质。

云平台的管理平台需提供全方位的云资源供给、运维和运营管理能力，具备一体化管控、智能化运维、精细化运营及个性化扩展等能力

容器服务为政务云平台提供容器集群管理、应用管理、镜像管理、告警监控管理、网络管理、存储管理等基本服务。通过容器服务，政务云平台的租户包括研发、运维人员可快速申请到软件运行的运行环境，结合开发运维一体化等技术，可以充分的将研发人员从部署运维中解耦出来。同时，多集群、镜像、告警监控等功能为应用的运行的提供了一套自动化流程，解决应用的版本管理，上云等问题。

云平台提供主流操作系统软件服务，包含操作系统的安装、维护等，提供授权数量满足政务云业务系统的使用需求。

公共资源交易平台技术专用

数据库服务按照兼顾现有系统现状，满足未来长期国产化演进的思路进行规划，可提供MySQL、SQLServerOracle等常见数据库，以及达梦等国产数据库服务。

提供云原生、湖仓一体的企业级大数据云服务，提供分析所需的 Kafka、CDL、Hudi、ClickHouse、HetuEngine、Flink、YARN、IoTDB、Ranger、Elasticsearch、Redis、Hive、Spark、HBase、Doris、CES、RTD 等组件，支持大规模集群滚动升级，并具有多租户、弹性伸缩、存算分离等企业级能力。支持实时计算，离线计算，分析计算，提供搜索引擎。

基于云平台提供虚拟桌面应用，实现高效的桌面远程连接协议，基于该协议用户可以通过瘦终端远程连接其在云平台的虚拟桌面，桌面的图像可以高效投送至远端的显示器上，而远端终端上的外设可以方便地基于各种策略映射至云平台的虚拟桌面上，实现用户桌面的卓越体验效果，满足不同场景用户办公诉求，使能客户办公系统数字化。

3.1.3.2 **服务需求分析**

3.1.3.2.1 计算建设需求

弹性云主机服务：提供由 CPU、内存、镜像、云硬盘组成，可随时获取、弹性可扩展的计算服务器，同时可以结合 VPC、安全组、数据多副本保存等能力，打造高效、可靠、安全的计算环境，支撑服务持久稳定运行。支持虚拟机设备直通，用户申请虚拟机时，可以申请将 USB、GPU、SSD 等设备映射给虚拟机使用。支持通用型，GPU 加速型等云主机创建，删除等生命周期管理。

裸金属服务（物理机）：提供专属的物理服务器，满足核心应用场景对高性能、稳定性、高安全性的需求。发放后的裸金属服务器可以与 VM 网络互通。用户可以通过管理平台申请裸金属服务，支持配置裸金属的 OS、IP 地址、登录 OS 的用户密码、安全组、需要绑定的弹性 IP 以及指定服务器发放完成后登陆信息，同时可以在申请时为裸金属增加多块数据盘，并设置部分数据盘为共享盘。

镜像服务：提供简单方便的镜像自助管理功能。用户可以灵活便捷的使用公共镜像、私有镜像或共享镜像申请弹性云服务器和裸金属服务器。同时，用户还能通过已有的云服务器或使用外部镜像文件创建私有镜像。

弹性伸缩服务：提供弹性伸缩服务，根据用户的业务需求和预设策略，自动调整计算资源，使云服务器数量自动随业务负载增长而增加，随业务负载降低而

公共资源交易平台投标专用

减少，保证业务平稳健康运行，降低人为反复调整资源以应对业务变化和高峰压力的工作量，节约资源和人力成本。

南阳政务云平台云平台所提供的计算服务不低于以下标准：

类型	名称	说明	规格
计算	云主机（GPU 基础版）	提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不低于 128bits。（直通型）	8 核 32G
		提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不低于 128bits。（虚拟化）	8 核 32G
	云主机（GPU 标准版）	提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G*2 GDDR6 显存、位宽不低于 128bits。（直通型）	16 核 64G
		提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G*2 GDDR6 显存、位宽不低于 128bits。（虚拟化）	16 核 64G
		提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G*1 显存、位宽不低于 256bits。（直通型）	16 核 64G
		提供 V100 卡或同档显卡，提供高性能图形计算加速，提供	16 核 64G

公共资源交易平台投标专用
AE2C19CEC7648E1A624B2688EA14DB9

		不低于 32G*1 显存、位宽不低于 256bits。（虚拟化）	
	云主机（GPU 高级版）	提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G*4 GDDR6 显存、位宽 不低于 128bits。（直通型）	32 核 128G
		提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G*4 GDDR6 显存、位宽 不低于 128bits。（虚拟化）	32 核 128G
		提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G*2 显存、位宽不低于 256bits。（直通型）	32 核 128G
		提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G*2 显存、位宽不低于 256bits。（虚拟化）	32 核 128G
	物理机（计算型）	2 路	单 CPU>=10 核，Mem>=64G,本地硬盘(SAS 盘)>=600G*2
			单 CPU>=10 核，Mem>=128G,本地

公共资源交易平台投标专用
AE2C19CEC7C46E1A62A8B2B88EA14DB9

			硬盘(SAS 盘)>=600G*2
			单 CPU>=10 核，Mem>=192G,本地硬盘(SAS 盘)>=600G*2
			单 CPU>=10 核，Mem>=256G,本地硬盘(SAS 盘)>=600G*2
			单 CPU>=10 核，Mem>=384G,本地硬盘(SAS 盘)>=600G*2
			单 CPU>=10 核，Mem>=512G,本地硬盘(SAS 盘)>=600G*2
			单 CPU>=10 核，Mem>=128G,本地硬盘(SAS 盘)>=600G*2
		4 路	单 CPU>=10 核，

公共资源交易平台投标专用
AE2C19CEC7646E1A62A8BC88FA1A0B9

			Mem>=192G,本地硬盘(SAS盘)>=600G*2
			单 CPU>=10核，Mem>=256G,本地硬盘(SAS盘)>=600G*2
			单 CPU>=10核，Mem>=512G,本地硬盘(SAS盘)>=600G*2
	GPU 卡	物理机叠加，单卡提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16GGDDR6 显存、显存位宽不低于 256bits。	块
		物理机叠加，单卡提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G 显存，位宽不低于 256bits。	块

公共资源交易平台投标专用
AE2C19CEC...

3.1.3.2.2 存储建设需求

云硬盘（共享存储）：提供虚拟块存储服务，主要给弹性云服务器和裸金属服务器提供块存储空间。像使用传统服务器硬盘一样，用户可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据做持久化存储。具备多挂 载点、高并发性、高性能、高 可靠性等特点。支持高，中，低 IO 云硬盘创建，支持 SATA,HDD，SSD 等存储介质，支持集中式 FC SAN 存储，支持分布式存

储，主要应用于需要支持集群、HA（High Available，指高可靠集群）能力的关键企业应用场景。

弹性文件服务：为用户的弹性云服务器（ECS）提供一个完全托管的共享文件存储，符合标准文件协议（NFS、CIFS），能够弹性伸缩至 PB 规模，具备可扩展的性能，为海量数据、高带宽型应用提供有力支持。支持 SATA,HDD 低 IO 存储介质。

对象存储服务（视频存储）：提供对象存储服务，能够为镜像文件、数据库备份文件、非结构化对象（如文件、图片、视频等）提供数据存储能力，包括：创建、修改、删除桶，上传、下载、复制、修改、删除对象等。支持对象语义、文件语义、HDFS 等多种协议。支持视频存储。支持 SATA,HDD 低 IO 存储介质。

南阳政务云平台云平台所提供的存储服务不低于以下标准：

类型	名称	说明	规格
存储	低 IO	适用于云硬盘、文件存储、对象存储，介质为 SATA,HDD，30MB/s< 吞吐量 <40MB/s，100<IOPS<1000。	TB
	中 IO	适用于云硬盘,介质为 SAS 盘 HDD,40MB/s<吞吐量 140MB/s，1000<IOPS<5000	TB
	高 IO	适用于云硬盘，介质为 SSD 盘，140MB/s< 吞吐量 <300MB/s，5000<IOPS<25000	TB
	视频存储		TB
	共享存储	适用于共享云硬盘，具备多挂载点、高并发性、高性能、高可靠性等特点。主要应用于需要支持集群、HA（High Available，指高可靠集群）能	TB

公共资源交易平台投标专用

		力的关键企业应用场景，多个云服务器可同时访问一个共享云硬盘，FC-SAN 存储空间，介质为 SAS 盘 HDD	

3.1.3.2.3 备份建设需求

对于一般数据，需要对数据进行实时备份，一定时间周期内全量备份，一般按天增量备份。对于重要数据，则需要进行实时备份，数据基本不会因故障而丢失；

数据备份服务需支持 Linux/国产操作系统，满足对 32/64 位系统平台及应用支持，兼容主流数据库、应用中间件的实时复制、加密、断点续传等，满足 IT 系统复杂性和兼容性需求；支持以多租户方式提供，支持租户自定义备份策略、恢复策略、备份任务管理，具有便捷易用的操作界面。

虚拟机/文件备份：为弹性云服务器提供整机备份，需要支持本地备份以及对备份数据的远程复制，并支持利用备份数据恢复云服务器数据，最大限度保障用户数据的安全性和正确性，确保业务安全。支持本地备份及异地备份。

数据库备份：在需要保护的生产服务器上安装统一备份客户端，并连接管理控制台。统一备份客户端将识别生产服务器中的数据库数据，并通过备份 API 读取生产服务器中的文件数据，然后将其传输至统一备份的介质服务器中，完成备份。统一备份的管理控制台是整个备份系统的纽带，负责向客户端软件和介质服务器发送控制信息，管理整个备份任务的运行。

云硬盘备份服务：为云硬盘提供备份功能，需要支持本地备份以及对备份数据的远程复制，并支持利用备份数据恢复云硬盘数据，最大限度保障用户数据的安全性和正确性，确保业务安全。

统一备份服务：为云应用到存储数据的全面保护、统一管理保护全栈云上业务，实现云主机、数据库、对象/文件存储、大数据的统一备份。支持本地备份及异地备份。

南阳政务云平台云平台所提供的备份服务不低于以下标准：

类型	名称	说明	规格
数据备份	虚拟机/文件备份	本地备份	TB
		异地备份（定时）	TB
		异地备份（实时）	TB
	数据库备份	本地备份	TB
		异地备份（定时）	TB
		异地备份（实时）	TB

3.1.3.2.4 网络建设需求

弹性负载均衡：弹性负载均衡将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

虚拟私有云：提供虚拟私有云（Virtual Private Cloud，VPC）服务，用户可在云中虚拟出一个私有的应用运行环境和安全域。构建隔离的、用户自主配置和管理的虚拟网络环境，提升云资源的安全性，简化用户的网络部署。用户可以自行创建自己要的多个网段，指定每个要创建的网络的网段、掩码、DNS 等，也可以指定这个网络内的路由规则以及 NAT 规则。

安全组：安全组用来实现组和组间的访问控制，将虚拟机加入安全组后，可对进出虚拟机端口的网络报文进行限制的安全过滤规则。关联虚拟机端口与安全组后，该安全组的规则会对进出该虚拟机端口的网络报文进行过滤，只有规则允许的报文才能通过。

VPN：虚拟私有网络，提供端到端的私有访问通道。远端用户和虚拟私有云之间通过 IPSec VPN（Internet Protocol Security Virtual Private Network）建立一条安全加密的通信隧道，使远端用户可以安全的直接访问 VPC 中路由网络内的业务资源。

网络 ACL：提供子网级别的安全防护，根据与子网关联的入站/出站规则，判断数据包是否允许流入/流出关联子网。

弹性 IP：提供从公网访问云数据中心内虚拟机的能力，弹性 IP 业务需结合虚拟机或负载均衡业务使用，用户可以自主将申请的公网 IP 绑定到虚拟机或者负载均衡器上，从而实现将云数据中心的业务开放到公网。

云专线：构建本地数据中心到虚拟私有云之间高速、低时延、稳定安全的专属连接通道，充分利用云计算优势的同时，继续使用现有的 IT 设施，实现灵活一体、可伸缩的混合计算环境。

NAT 服务：提供 NAT 服务，能够为 VPC 内的弹性云服务器提供 SNAT 和 DNAT 功能，通过灵活简易的配置，即可轻松构建 VPC 的一体化业务出入口。

SNAT 是源 NAT（源地址转换）。内部地址要访问外网上的服务时，内部地址会主动发起连接，由路由器或者防火墙上的网关对内部地址做个地址转换，将内部地址的私有 IP 转换为外网 IP，网关的这个地址转换称为 SNAT，主要用于内部共享 IP 访问外部。

DNAT 是目的 NAT（目的地址转换）。当内部需要提供对外服务时（如对外发布 web 网站），外部地址发起主动连接，由路由器或者防火墙上的网关接收这个连接，然后将连接转换到内部，此过程是由带有外网 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。

云解析：提供高可靠，高扩展的权威 DNS 服务和 DNS 管理服务，将域名或应用资源转换成用于计算机连接的 IP 地址，从而将最终用户路由到相应的应用资源上。

二层桥接：提供云内 VM 与云外的虚拟化资源池及外部网络进行二层互通能力，实现业务迁移上云 IP 地址不变、同一云外云内云外部署二层互通。

VPC 终端节点：提供同区域下跨 VPC 连接，实现 VPC 间的资源通信。提供在 VPC 内提供与支持终端节点服务（专线/VPN/容器）进行连接，该服务使用云内部网络，无需弹性公网 IP。（通过在 VPC 中创建应用程序并将其配置为终端节点服务，同一区域下其他 VPC 内创建的终端节点可以与该终端节点服务建立连接，进行通信。）

云连接：提供快速构建同区域或者跨区域多个 VPC 间互通的能力：当云上多个区域的 VPC 之间需要跨区域进行私网通信时，利用云连接可以根据网络规划，实现多个跨区域 VPC 连通。

南阳政务云平台云平台所提供的网络服务不低于以下标准：

公共资源交易平台技术专用

类型	名称	说明	规格
负载均衡	虚拟负载均衡		

3.1.3.2.5 操作系统建设需求

云平台提供的弹性云主机服务需支持客户提供的 windows server，linux server 作为 guestOS，guest OS 支持从私有镜像，共享镜像，公共镜像创建弹性云主机。

统信服务器操作系统基于 Linux 稳定内核研发，集成了资源管理、运维管理、和 DDE 桌面环境等标准系统组件，以及服务管理、中间件、WEB 服务、办公服务等应用服务组件。它还适配了大量的第三方开源、商业闭源等软件和解决方案，适用于多种应用场景。

银河麒麟高级服务器操作系统是针对企业级关键业务，依据 CMMI5 级标准研制的提供内生安全、云原生支持、国产平台深入优化、高性能、易管理的新一代自主服务器操作系统；同源支持飞腾、鲲 鹏、龙芯、申威、海光、兆芯自主平台；可支撑构建大型数据中心服务器高可靠集群、负载均衡集群、分布式集群文件系统、虚拟化应用和容器云平台等，可部署在物理服务器和虚拟化环境、私有云、公有云和混合云环境。

红帽 Linux 是一款兼具稳定性、可靠性和安全性的高性能操作系统，通过全面的内核、驱动程序和网络协议更新，为现代 IT 环境提供了卓越的价值。该系统具备出色的兼容性和可扩展性，支持广泛的硬件设备和外置设备，并适应了未来网络发展趋势。同时，红帽 Linux 6 注重用户体验和易用性，提供了一系列精心设计的应用软件，满足用户在各种场景下的需求。

Windows Server 是一款适用于企业级应用的服务器操作系统，具有广泛兼容性、强大性能和易管理性等特点。它提供了友好的用户界面和可伸缩的基础结构，支持多种应用程序和服务，并且具备虚拟化技术，可以提高服务器的利用率和效率。同时，Windows Server 还提供了多项安全性功能，保障企业网络的安全性。管理员可以使用良好的管理和维护工具，如活动目录、远程桌面服务和网络访问保护等，方便地进行管理和维护。Windows Server 还适应不同的企业应用场景，

无论是文件共享、打印服务、Web 服务器还是小型企业网络等场景，都可以得到满足。

南阳政务云平台云平台所提供的操作系统服务不低于以下标准：

类型	名称	说明	规格
操作系统	Linux Server	根据需要提供合适的版本（包括国产操作系统）	实例
	Windows Server	根据需要提供合适的版本	实例

3.1.3.2.6 数据库建设需求

关系型云数据库MySQL：提供基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线云数据库服务。提供完善的性能监控体系和多重安全防护措施，并提供了专业的数据库管理平台， 让用户能够在云上轻松的进行设置和扩展云数据库。通过云数据库服务的管理控制台，用户无需编程就可以执行所有必需任务，简化运营流程，减少日常运维工作量，从而专注于开发应用和业务发展。

关系型云数据库Oracle： 支持创建异地灾备库，通过数据传输实现异地数据实时同步，在突发状况下，用户可将异地灾备库切换为主库，保障业务可用性。具有强的容错能力、错误恢复能力、错误记录及预警能力，能在不影响数据库运行的条件下快速恢复已提交的修改。可以在秒级别将整个数据库、表、表中的记录或是事务恢复到指定时间点。支持存储过程、触发器。触发器支持语句执行前、执行后和可替换型三种方式。支持行级触发器。触发器的触发操作和事件包括DML、DDL、数据库启停、错误信息、登录/注销。支持大规模数据加载和更新，数据库的数据文件能跨平台互相交换。

关系型云数据库SQL Server：支持数据定义、数据操纵、数据完整性保障、数据备份和恢复、事务处理、安全性管理、多用户并发控制、数据复制、OLAP技术以及XML等多个功能特性。同时高可靠性选项，以确保数据的可用性和完整性。此外，需支持移动性和集成，可以轻松地与移动设备和云服务集成，以满足现代企业的需求。

缓存数据库 Redis：提供即开即用、安全可靠、弹性扩容、便捷管理的在线分布式缓存能力，满足用户高并发及数据快速访问的业务诉求。提供多类型的实例架构，包括单机架构、主从架构、集群高可靠架构。安全的数据管理：支持数据备份恢复及数据持久化等，以保障数据的高可靠性。便捷的运维管理：具备高可靠部署能力，同时支持管理中心下发的应用对内存数据库的适配。

关系型数据库 PostgreSQL：支持 NoSQL 数据类型（JSON/XML/ hstore），支持企业复杂查询 SQL 的 OLTP 业务场景，提供 PostGIS 地理信息引擎、多维多模时空信息引擎。需具备高可靠部署能力。

分布式关系型数据库：基于 Shared-Nothing 架构，它是由众多拥有独立且互不共享 CPU、内存、存储等系统资源的逻辑节点组成。在这样的系统架构中，业务数据被分散存储在多个计算节点上，数据查询任务被推送到数据所在位置就近执行，通过协调节点的协调，并行地完成大规模的数据处理工作，实现对数据处理的快速响应。基于普通服务器和横向扩展 的方式，构建支持海量数据存 储和访问的数据库系统，从而实现无线扩容和弹性扩展。

分布式文档数据库：采用存算分离架构，提供分库分表、弹性扩容等能力，具有稳定可靠、高度可扩展、持续可运维的特点。服务器集群管理对用户完全透明，用户通过管理控制台进行数据库运维与数据读写，提供类似传统单机数据库的使用体验。提供稳定可靠、可弹性伸缩的在线数据库服务，是一种高安全、高可靠，易运维的数据库，提供备份、恢复、监控服务等基 本功能，配合提供数据库基础运维服务。

国产数据库：

- **达梦数据库**：具备强大的数据处理和分析能力，支持丰富的数据管理和控制工具，以确保数据的完整性和可靠性。它能够高效地处理大量数据，并提供实时分析功能，帮助企业快速做出决策。此外，支持各种先进的数据库管理功能，如数据分区、数据压缩、全文检索等，以提高数据管理效率。具备高可靠性和可扩展性，以确保数据的可用性和完整性。如支持自动备份和恢复、故障切换等，以最大程度地减少数据丢失和停机时间。此外，需支持水平扩展和垂直扩展，可以轻松地满足企业不断

增长的数据需求。提供租用、安装、调优、排错、技术支持。

- **人大金仓KingbaseES数据库：**支持高效的数据存取和查询性能，适用于大规模的数据处理和实时分析。支持多种安全机制，包括用户认证、访问控制、数据加密等，保障数据的安全性和隐私性。支持多种数据类型，包括字符型、数值型、日期型、二进制型等，方便用户进行数据管理和处理。支持多种操作系统和硬件平台，可以灵活地部署在不同的服务器和云平台。提供租用、安装、调优、排错、技术支持。
- **南大GBase 8a MPP Cluster数据库：**支持联邦构架、大规模并行计算、海量数据压缩、 高效存储结构、智能索引、虚拟集群及镜像、灵活的数据分布、完善的资源管理、在线快速扩展、在线节点替换、高并发、高可靠性、高安全性、易维护、 高效加载等技术特征。 提供租用、安装、调优、排错、技术支持。

南阳政务云平台云平台所提供的数据库服务不低于以下标准：

类型	名称	说明	规格
云数据库	关系型数据库	提供稳定可靠、可弹性伸缩的在线数据库服务，是一种高安全、高可靠，易运维的 MySQL 数据库，提供备份、恢复、监控服务等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存储另行计费。	2 核 4G，最大连接 数： 1200
			4 核 8G，最大连接 数： 2000
			8 核 16G，最大连接 数： 4000
			16 核 64G，最大连接 数： 16000
			32 核 128G，最大连 接数： 20000

公共资源交易平台投标专用
4E2C19CEC7646E1A62A8BC88EA14DB9

		关系型数据库 Oracle，提供安装与激活服务，提供数据库基础运维服务。	数据库实例
		SQL Server 拥有高可靠架构和数据恢复功能，包含 License 授权，支持实例管理、账号管理、数据库管理、白名单、备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存储另行计费。	2 核 4G
			2 核 8G
			4 核 16G
			8 核 16G
			8 核 32G
			16 核 32G
		缓存数据库 Redis，提供数据监控、数据管理、数据安全、备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存储另行计费。集群版： 主从版*2	主从版-2G
			主从版-4G
			主从版-8G
			主从版-16G
			主从版-32G
			主从版-64G
			集群版-16G
			集群版-32G
			集群版-64GB
		关系型数据库 PostgreSQL，配合提供数据库基础运维服	2 核 4G，最大连接数 1200，最大 IOPS 2500
			2 核 8G，最大连接数 1600，最大 IOPS 3500
			2 核 16G，最大连接数 2500，最大 IOPS 4500

公共资源交易平台投标专用
AE2C19CEC7764CH1624B3B88

			4 核 16G，最大连接数 4000，最大 IOPS 7000
			4 核 32G，最大连接数 5000，最大 IOPS 9000
			8 核 64G，最大连接数 10000，最大 IOPS 18000。
			16 核 128G，最大连接数 12000，最大 IOPS 36000
	分布式关系型数据库	基于普通服务器和横向扩展的方式，构建支持海量数据存储和访问的数据库系统，从而实现无线扩容和弹性扩展。	2 核 8G，最大连接数 1600，最大 IOPS 3500
			2 核 16G，最大连接数 2500，最大 IOPS 4500
			4 核 16G，最大连接数 4000，最大 IOPS 7000
			4 核 32G，最大连接数 5000，最大 IOPS 9000
			8 核 64G，最大连接数 10000，

公共资源交易平台投标专用
AE2C19CEC7646E1A62A8BC88EA14DB9

			最大 IOPS 18000。
			16 核 128G，最大连接数 12000，最大 IOPS 36000
	分布式文档数据库	基于分布式文档数据库，提供稳定可靠、可弹性伸缩的在线数据库服务，是一种高安全、高可靠，易运维的数据库，提供备份、恢复、监控服务等基本功能，配合提供数据库基础运维服务。	2 核 8G
			4 核 16G
			8 核 32G
			16 核 64G
	国产数据库	提供不少于三种国产数据库，提供租用、安装、调优、排错、技术支持。	1CPU

3.1.3.2.7 大数据建设需求

云原生数据湖：提供云原生、湖仓一体的企业级大数据云服务，提供分析所需的 Kafka、CDL、Hudi、ClickHouse、HetuEngine、Flink、YARN、IoTDB、Ranger、Elasticsearch、Redis、Hive、Spark、HBase、Doris、GES、RTD 等组件，支持大规模集群滚动升级，并具有多租户、弹性伸缩、存算分离等企业级能力。支持实时计算，离线计算，分析计算，提供搜索引擎。

实时计算：提供流式计算引擎，将各种不同的数据源中的数据进行实 时的订阅、处理、分析。

离线计算：服务于批量结构化数据的存 储和计算，可以提供海量数据 仓库的解决方案，存储另算。

搜索引擎： 提供数据分析、搜索等场景服务。

分析计算： 提供对海量数据进行即时的 多维分析透视和业务探索，快速构

公共资源交易平台技标专用

建数据仓库。

南阳政务云平台云平台所提供的大数据服务不低于以下标准：

类型	名称	说明	规格
大数据服务	实时计算	提供流式计算引擎，将各种不同的数据源中的数据进行实时的订阅、处理、分析。	1CPU+4G 内存
	离线计算	服务于批量结构化数据的存储和计算，可以提供海量数据仓库的解决方案，存储另算。	1CPU+4G 内存
	搜索引擎	提供数据分析、搜索等场景服务，存储另算。	1CPU+4G 内存
	分析计算	提供对海量数据进行即时的多维分析透视和业务探索，快速构建数据仓库，存储另算。	1CPU+4G 内存

3.1.3.2.8 容器建设需求

容器服务为南阳政务云平台提供容器集群管理、应用管理、镜像管理、告警监控管理、网络管理、存储管理等基本服务。通过容器云，影像平台的研发、运维人员可快速申请到软件运行的运行环境，结合开发运维一体化等技术，可以充分的将研发人员从部署运维中解耦出来。同时，多集群、镜像、告警监控等功能为应用的运行的提供了一套自动化流程，解决应用的版本管理，上云等问题。

容器服务：基于 Docker 容器和 Kubernetes 容器编排和调度技术，具备秒级扩容能力，可为企业应用提供编排、调度、部署、弹性伸缩、升级、自动化运维等基于容器的全生命周期管理能力。

容器镜像仓库：提供简单易用、安全可靠的镜像管理功能，可快速部署容器化服务。

服务网格：提供非侵入式微服务治理解决方案，支持完整的生命周期管理和流量治理，兼容 Kubernetes 和 Istio 生态，提供包括负载均衡、熔断、限流等多种治理能力。并内置金丝雀、蓝绿灰度发布流程，提供一站式自动化的发布管

公语言易平台技标专用

理。

南阳政务云平台云平台所提供的容器服务不低于以下标准：

类型	名称	说明	规格
容器服务	容器服务	提供灰度发布，多集群管理，支持 K8S 容器调度等应用服务能力。	

3.1.3.2.9 应用建设需求

ROMA Factory 是面向企业的一站式应用管理与运维平台，为企业开发人员、测试人员、运维人员或项目经理等角色，提供应用托管、监控、告警和日志分析等能力，同时平台极具开放性，兼容业界主流应用技术栈，包括：多种语言，多种微服务框架和多种运行环境，能帮助企业极大地提升传统应用、Web 应用、微服务应用的管理与运维效率，聚焦面向行业的应用创新，从而提升企业竞争力。

- 支持分布式服务框架、服务治理、统一配置管理、分布式链路跟踪、高可靠及数据化运营等。
- 支持弹性扩缩容能力，支持手动扩容，支持自动弹性伸缩功能。
- 支持界面化查看应用扩容流程，能够显示扩容详细流程，支持界面化查看扩容事件，正在执行扩容，扩容流程结束，显示详细应用从创建、拉取镜像、启动应用的全过程。
- 支持灰度能力，提供应用灰度发布功能。提供微服务故障隔离能力。提供注册发现、配置管理和分布式协调：支持 Nacos、ZooKeeper 或其他商业功能组件等。
- 提供故障容错能力：支持限流降级、故障隔离、健康检测等功能。
- 提供日志管理能力：支持基础微服务框架日志。
- 提供流量控制：支持基于请求数或并发数等指标的限流降级功能。
- 提供服务观测能力：支持可视化监测服务拓扑，链路追踪等。
- 支持弹性扩缩容能力，支持手动扩容，支持自动弹性伸缩功能，可以根据预置的策略（CPU 利用率或 RT 响应时间），自动触发应用的弹性伸缩。能够看到新扩容应用的 IP 地址及应用所在的节点。

- 支持界面化查看应用扩容流程，能够显示扩容详细流程，支持界面化查看扩容事件，正在执行扩容，扩容流程结束，显示详细应用从创建、拉取镜像、启动应用的全过程。
- 支持灰度能力，提供应用灰度发布功能。
- 提供微服务故障隔离能力，当应用故障报错，能够实现 3 秒钟隔离故障能力，不影响服务正常使用。
- 提供注册发现、配置管理和分布式协调：支持 Nacos、ZooKeeper 或其他商业功能组件等。
- 提供云原生网关和服务网格：支持 ServiceMesh，Istio，Http/https 协议，提供服务通讯安全认证、流量路由、流量拆分管理、网格可观测等功能。
- 提供微服务治理能力：支持 SpringCloud，包括微服务配置、服务发现、服务鉴权、故障隔离、流量监控、链路追踪、协议转换等功能。
- 提供流量控制：支持基于请求数或并发数等指标的限流降级功能。
- 提供故障容错能力：支持限流降级、故障隔离、健康检测等功能。
- 提供服务观测能力：支持可视化监测服务拓扑，链路追踪等。
- 提供日志管理能力：支持基础微服务框架日志。

南阳政务云平台云平台所提供的应用服务不低于以下标准：

类型	名称	说明	规格
应用服务	应用与数据集成服务	提供将物联网、大数据、视频、统一通信、GIS 等基础平台及各个应用的服务、消息、数据统一集成适配以及编排的能力。	
	应用管理	应用管理平台，提供资源及业务应用的实时监控、实时告警事件、统一日志收集和分析等功能。	

公共资源交易平台技术专用

	应用工厂服务	应用管理与运维平台为开发人员、测试人员、运维人员或项目经理等角色，提供应用托管、监控、告警和日志分析等能力提供以应用为中心的应用发布、部署、监控、告警、日志等一站式管理能力。	1VCPU/月
	应用迁移	系统迁移服务	1 虚机/次

3.1.3.2.10 网络及托管建设需求

随着互联网技术的不断发展，业务需求的多样性，单位或企业对数据存储和管理的要求越来越高。托管服务作为网络、服务器、硬件设备的一种解决方案，已经成为企业信息化建设的重要手段之一。南阳市政务云机房具备大规模的场地及配套设施，包括国标 5A 级 IDC 机房环境，系统化的监控手段和标准化的安全体系。能够确保托管设备的安全、稳定运行，并提供高速可靠的内外部网络环境，保证数据传输的效率和可用性。本项目可提供网络及托管服务，主要包括互联网带宽、互联网 IP 及设备托管等。

南阳政务云平台云平台所提供的网络及托管服务不低于以下标准：

类型	名称	说明	规格
网络及托管服务	互联网带宽	提供互联网访问独享带宽 2-100Mbps 部分，每 2 兆带宽 40 元，超过 100M 部分，每 2 兆带宽 34 元）	2Mbps
	互联网 IP	提供互联网 IP 地址，IPv4 版（IPv6 地址免费）	1 个
	设备托管	提供 1U 托管机位	1U

公共资源交易平台招标专用

		提供 42U 标准托管机架（3.5KW）	1 架

3.1.3.2.11 云桌面建设需求

基于云平台提供虚拟桌面应用，实现高效的桌面远程连接协议，基于该协议用户可以通过瘦终端远程连接其在云平台的虚拟桌面，桌面的图像可以高效投送至远端的显示器上，而远端终端上的[illegible]设可以方便地基于各种策略映射至云平台的虚拟桌面上，实现用户桌面的卓越体验效果，满足不同场景用户办公诉求，使能客户办公系统数字化。

南阳政务云平台云平台所提供云桌面服务不低于以下标准：

类型	名称	说明	规格
云桌面	云桌面	云桌面	提供云桌面授权，不含终端，支持软拨号。

3.1.3.2.12 业务迁移需求

随着应用、数据不断增多，服务器数量也逐年增加，服务器端在管理、日常维护方面的需求逐渐显现。针对业务不断发展导致服务器数量快速增加、维护工作量大、维护成本高、机房空间紧张等问题，政务云租户决定基于云计算等先进信息技术，深化信息系统硬件资源池建设规模，进一步提高硬件资源利用效率、节省机房空间、降低运营成本、加强硬件资源建设管控能力、提高应用系统部署效率，降低应用系统对物理服务器的依赖性，需要将现有 XX 系统迁移至南阳政务云平台。

应用上云服务是根据客户应用调研结果，结合客户对网络带宽、数据容量以及宕机时间的要求，制定迁移服务解决方案，帮助客户实现数据与应用上云的过程。具体迁移需求如下；

- 配合各单位应用系统迁移前的环境需求分析工作。
- 负责各单位应用系统迁移前的测试环境搭建工作。
- 配置物理服务器、配置虚拟机、配置网络、安装操作系统、配置相应的

公共资源交易平台投标专用

安全策略等。

- 配合或提供各单位应用系统迁移需要使用的迁移工具。
- 配合各单位应用系统迁移过程中遇到问题故障分析以及提出解决方案，并配合解决问题故障。
- 负责各单位应用系统迁移过程中对硬件、网络、软件、安全等运行环境的变更工作。
- 配合各单位应用系统迁移后进行测试工作，如压力测试、故障测试等。

3.1.3.2.13 云平台管理建设需求

3.1.3.2.13.1运营需求

一云多池：一套云平台支持同时接入多个不同 Region，提供统一管理可以方便租户快捷的申请使用不同 Region 下的云服务资源。这些 Region 内可以有多个不同类型资源池。

租户管理：运营管理员可为每个入驻的企业创建一个租户，并且缺省给每个租户开通一个一级 VDC。

服务目录：提供云服务目录管理能力。

服务管理：提供开箱即用的产品目录和产品，包括计算、存储、网络、安全、应用服务、数据库、企业应用等产品。支持运营管理员根据产品参数的固定和开放定义新的产品。

订单管理：提供订单审批能力，可以选择同意、驳回修改、拒绝并关闭、转他人审批。

审批流程管理：支持审批流程的创建、修改、删除、发布和取消发布，支持多级审批流程定义。最多支持 5 级审批。

计量计价：支持对所有租户的资源使用量进行统计，支持按规格指标计量和计价，支持租户内按 VDC 使用量计量、按 VDC 资源计量和按已删除 VDC 计量计价。

资源管理：支持对云服务实例打标签、纳管，并且支持按照标签进行过滤。

代维管理：支持跨一级 VDC 代维，代维账号可以进入被代维的多个一级 VDC 进行代维。

公告栏：租户面用户可以在首页查看管理员发布的公告。

公开资源云平台技术专用
AE2C19CE776482E1A62A8BC88EA14DB9

购物车：用户可以将需要申请的产品一次性放入购物车，从购物车直接提交申请。

回收站：支持用户删除资源后保留到回收站，允许误删除后恢复资源，支持资源冻结期设置，在冻结期内不允许彻底删除。

应用管理：支持租户进行应用分组管理能力。

项目管理：提供项目内创建资源列表信息。支持在项目中通过表格批量申请资源。

多级 VDC：VDC（虚拟数据中心）管理员可以在 VDC 内再划分多个子 VDC，灵活匹配用户的组织模型，VDC 可以支持 5 级 VDC 嵌套。统一门户：提供云平台统一门户，集中展示云服务市场，提供产品解决方案介绍。

运营北向 API：提供运营北向接口，包括：产品管理、订单管理、服务编排、计量计价、资源生命周期管理和 VDC 管理等接口。

3.1.3.2.13.2**运维需求**

告警管理：支持当前告警、历史告警、事件查询和导出；支持告警屏蔽、归并和抑制、重定义、自动确认；支持告警远程通知。

监控管理：支持对云平台的各类物理虚拟资源进行监控，提取各类资源的监控指标，并支持设定阈值产生相应的阈值告警。

运维管理员账号管理：提供运维管理员账号管理，提供运维管理角色管理能力，内置管理员和安全管理员等角色。

日志管理：提供运维侧管理日志和租户操作日志的统一汇聚和查询。

CMDB：提供数据中心统一的资源信息中心，通过资源自动发现、模板导入多种方式发现资源，支持给资源打标签，支持给资源管理位置信息，支持资源导入导出功能。

容量管理：提供计算、存储、网络等基础资源的容量信息和容量使用的历史趋势，并预测容量瓶颈。

多云监控：支持省级云集中运维市级云，统一呈现市级云资源、告警、容量汇总数据。一个省级云可以对接多个市级云。

运维自动化：运维自动化解决日常运维过程中重复多次、流程固定且繁琐的操作难题，支持批量对云资源下发脚本执行，完成批量修改密码、批量打补丁等

公共资源交易平台投标专用

运维动作。

拓扑管理：自动发现数据中心内网络设备之间的网络链路，自动生成物理设备之间的网络拓扑视图，建立物理拓扑到虚拟网络拓扑的关联。叠加关键的运维指标如告警数据。支持拓扑编辑，辅助完善拓扑视图。

应用监控：支持运维管理员以应用的视角进行监控与分析，支持运维管理员手工创建应用，并将应用与对应的资源对象进行关联，通过对应用关联的资源对象性能指标以及告警进行综合评估，提供应用的繁忙度与健康度。

闲置/瓶颈资源分析：通过对资源对象性能指标的分析，获取资源池中闲置资源以及瓶颈资源，供运维管理员提供整体资源池的利用率，并及时发现瓶颈风险。

消息通知服务：提供可靠，可扩展，海量的消息通知服务。简化系统的耦合，能够根据用户的需求，向订阅者主动推送消息的服务，订阅者可以是电子邮件，短信，应用等等。

统一密码管理：支持对云平台各服务的人机密码、机机密码进行统一管理。

统一证书管理：提供云平台周边部件的证书管理能力。实现部件证书即将过期提示，证书批量更新，失败部件证书单独更新能力。

统一巡检：支持对云平台包括 ManageOne 自身进行巡检，输出巡检报告。

系统维护：提供对 ManageOne 自身的维护配置等操作。

运维北向 API：提供了运维北向 Rest 接口，允许第三方网管系统可以从运维侧抽取所管数据中心的资源、告警和性能数据。告警提供 Rest 抽取和 SNMP 主动上报两种方式，SNMP 方式支持告警上报筛选能力。

3.1.3.3 安全需求分析

安全部分满足租户安全需要，满足但不仅限以下服务内容，保证政务业务系统的网络安全、数据安全等。

类别	名称	技术指标
云安全	虚拟防火墙	提供虚拟网络安全区域边界安全防护能力。
	虚拟漏洞扫描	提供虚拟化漏洞扫描功能，包含数据库漏洞扫描、系统漏洞扫描、WEB 漏洞扫描、主机基线配

公共资源交易平台技术专用

	置核查、网络基线配置核查等功能模块，提供报告。
虚拟堡垒机	提供虚拟化运维安全管理与审计系统(堡垒机)安 全能力
虚拟主机安全	虚拟机形态部署，提供资产管理、安全体检、安全监控、漏洞风险、入侵威胁、合规基线等多个功能模块，各个模块进行联动，模块间数据联通，形成闭环系统，为企业提供强有力的采集、检测、监测、防御、捕获能力，对主机进行全方位的安全防护。
虚拟 Web 应用防火墙	提供虚拟化 WAF 安全能力。
网页防篡改	提供网页防篡改功能。
虚拟日志审计	提供日志分析系统，支持日志的采集、过滤、归并、关联分析、展现、告警监控、实施事件监控、报表等。
虚拟 VPN 安全接入	提供国密 SSLVPN 加密服务，移动办公安全接入，包括接入用户身份认证、传输数据加密、权限划分和接入审计，每 100 个 VPN 并发组件。
虚拟防病毒	提供虚拟化防病毒能力。
入侵检测	整机吞吐量≧10Gbps。
虚拟数据库审计	针对用户对数据库的访问行为进行记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源。加强内外部数据库网络行为记录，提高数据资产安全。
虚拟密码机	能够为政务云提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，可以满足通用密码服务，保证传输

公共资源交易平台投标专用
AE2C19CEC7C4CE1AC2A8DC88EA14DB9

		信息的机密性、完整性和有效性，司时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。
	数据库加密服务	200 实例。

3.1.3.3.1 平台安全需求

云平台安全风险包括传统网络安全以及云化后新引入的安全风险两部分，传统安全风险涵盖物理层、网络层、主机层、应用层、数据层风险，使用云计算模式后引入了新的资产，安全风险包括涵盖物理和环境安全、网络和通信安全、设备和计算安全，应用和数据安全，涵盖了宿主机、虚拟化层、虚拟化网络、云主机、应用层、数据层、用户层。

1、物理和环境安全风险

主要包括物理灾害、物理访问控制、基础设施安全风险。

2、网络层和通信安全风险

主要包括：网络可用性风险、边界完整性风险、安全通信风险、入侵防护风险、恶意代码风险。

3、宿主机风险

包括外设与固件安全风险。

4、虚拟化平台风险

主要包括虚拟化逃逸、平台自身可信、资源恶意竞争、虚拟机镜像安全风险。

虚拟化网络边界

主要包括边界模糊、边界动态弹性、虚拟化流量不可见、多租户、虚拟机漂移等风险。

5、虚拟主机安全风险

主要包括：操作系统漏洞、恶意代码、终端管控、审计等风险。

6、应用安全风险

主要包括：应用服务可用性风险、WEB 攻击风险、API 等安全风险。

7、数据安全风险

公共资源交易平台投标专用

包括：数据使用、数据存储、数据传输、数据备份、恢复风险、数据迁移、数据残留风险。

按照网络安全等级保护最新要求，云服务商需要满足全部《安全通用要求》和《云计算测评扩展要求》中适用于云计算平台部分的指标，通过建设为云上使用者提供可信、可靠的安全环境。

3.1.3.3.2 租户安全需求

租户侧需要考虑主机系统、应用系统安全风险，具备发现漏洞和资产核查能力，需要具备恶意代码防范能力，对外提供的 web 服务能力需要具备检测和防御 web 攻击的能力。需要具备云主机远程安全运维管理能力，日志审计能力，数据库审计能力等。

一、监测类安全能力

（1）虚拟漏洞扫描

漏洞扫描系统应具有以下层面功能：

- 主机扫描：主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。全方位检测信息系统存在的主机、软件的安全漏洞，安全配置问题，弱口令，不必要开放的账户、服务、端口，独创的端口识别技术，结合信息丰富的协议指纹库，能自动快速准确的识别出非标准开放端口和应用服务类型，准确扫描端口对应的服务漏洞，极大避免扫描过程中的漏报和误报。
- 网站扫描：全面支持 OWASP_TOP10 检测，可以帮助用户充分了解 Web 应用存在的安全隐患，建立安全可靠的 Web 应用服务，改善并提升应用系统抗各类 Web 应用攻击的能力（如：注入攻击、跨站脚本、文件包含、钓鱼攻击、信息泄漏、恶意编码、表单绕过等），协助用户满足等级保护、PCI、内控审计等规范要求。
- 数据库扫描：数据库扫描模块可帮助用户充分了解数据库存在的安全隐患，通过定期数据库系统安全自我检测与评估，提升用户各类数据库的抗风险能力。同时可以协助用户完成数据库建设成效评估，协助数据库安全事故的分析调查与追踪。
- 基线核查：全面覆盖操作系统、数据库、中间件、防火墙、路由器、交

公共资源云服务平台投标专用

换机等设备类型，支持 Windows 下的离线检查，无需一台台设备建立任务，一键提取系统配置信息，并可导入远程安全评估系统出具修复加固建议报告。

（2）网站监测

网站监测系统应具有以下功能：

- 网站可用性监测：对网站进行 7*24 小时监测，发现访问异常（包括访问通断、访问响应太慢）时，及时向用户进行短信和邮件的告警。多个监测点排除了因监测线路、运营商等问题造成的误报，极大的保证了监测结果的准确性。
- 网站内容监测：

1）文本内容监测

违规文本识别：基于文本匹配识别、文本语义分析、自然语言处理、图文提取识别等技术识别发现违规文本。

违规图像识别：基于智能图像识别、图像目标识别、图像人脸识别、图像样例识别等技术识别发现违规图像。

快速网址检测：基于黑白名单网址快速检测技术识别发现违规业务。

2）篡改监测

实时对网站进行网页篡改监控，监测用户指定页面的内容和结构变化。发现变更后，系统首先向运维人员告警。运维人员核实变更事件是恶意篡改还是网站正常更新。如为恶意篡改，立即通过电话、短信和邮件向用户告警。

3）网页挂马监测

网站被恶意植入木马程序后，可能造成账号密码等敏感信息被窃取泄露等；挂马监测对客户网站系统进行7×24小时监测，发现网站系统中被恶意植入木马程序后，及时向用户告警，使网站管理员能够第一时间得知自己网站的安全状态，及时清除网页木马，避免给访问者带来安全威胁，影响网站信誉。

4）敏感关键字监测

监测网站页面中是否存在敏感信息（政治、色情、反党、反人类的关键词），及时告警，使得网站管理员可以及时删除敏感内容，避免事件影响扩散，给自身带来声誉和法律风险。用户也可以自定义关键词。

公共资源交易平台投标专用

5）暗链检测

检测网站是否被嵌入暗链地址，一般为在浏览器中隐藏不可见的网站链接，如网游、博彩，色情等广告链接，发现暗链后，及时向客户进行告警。

二、防护类安全能力

（1）虚拟 Web 应用防火墙

Web应用防火墙用于防护SQL注入、XSS、命令注入等各类Web攻击和威胁，应针对应用层HTTP/HTTPS协议进行安全防护。

Web应用防火墙应满足以下要求：

- 支持 HTTP 协议规范性检查；
- 支持对用户提交的 URL、参数、Cookie 等字段进行检查，采用 SQL 语义解析技术防止风险系数极高的 SQL 注入攻击，采用字符偏移技术对代码、命令、文件、LDAP、SSI 等注入攻击的检测；
- 采用字符差分技术对用户提交的脚本进行检查，防止不合法跨站脚本
- 采用行为识别算法有效识别扫描器或黑客持续性攻击，避免被扫描器持续猜测攻击或黑客持续渗透攻击。
- 支持对 Web 服务器容器、应用中间件、CMS 系统等漏洞进行有效防护。

（2）虚拟主机安全

应向用户提供主机系统防护与加固、主机网络防护与加固等功能，应具备勒索病毒专防专杀、东西向流量微隔离、补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力，提升终端安全防护水平。

主机安全类产品应满足以下要求：

- 支持强力查杀功能，对于无法普通隔离的病毒文件强制停止进程并隔离或动态移除到删除队列。支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用。
- 对不同的业务之间的流量进行精准识别、针对非法流量可以精准阻断。
- 提供策略级异常进程监控能力。
- 具备文件完整性监控功能，监控指定监控目录下内容完整性
- 能阻断对 SSH 和 RDP 暴力破解行为。

公共资源交易平台投标专用

（3）网页防篡改

网页防篡改应提供如下功能：

- 网页文件保护

通过web防攻击模块、防篡改模块（系统内核层的文件驱动），可对动态和静态网页文件进行完美的保护。按照用户配置的进程及路径访问规则，设置网站目录、文件的读写权限，限制文件目录的增、删、改操作行为，确保网页文件不被非法篡改。

- 集中管理

通过监控端集中管理多台Web服务器，监测多主机实时状态，制定保护规则，接收Web服务器的报警和日志信息。控制Web服务器的启用、关闭、禁用等状态，并可对Web服务器的日志和报警情况做统计分析。

- 实时报警

对非法篡改行为，系统会自动记录报警日志，并通过手机短信、电子邮件、syslog等多种方式通知管理员。能对网站攻击做到快速响应，及时应变。

- 管理员权限分级

可对管理员及监控端分配不同的权限组合。

- 日志审计

提供管理员行为日志，包括：时间、事件、操作对象、行为、IP地址等详尽信息，方便区分正常更新过程还是篡改攻击行为；支持保护日志查询审计功能；用户不能进行日志修改、删除操作，确保日志的准确性与完整性。

- 站点文件保持

防篡改模块集成在Web服务器软件中，通过设定各种站点文件访问过滤规则，对多个站点文件或单个站点的文件夹进行保护。

- 系统信息检测

管理控制端机器能记录所有监控端Web服务器的CPU、内存、硬盘等应用情况，方便管理员根据提供的硬件信息做升级和维护调整。

- 系统自我保护

公共资源交易平台投标专用

网页防篡改系统能够实时地保护自己，不被非法的删除、修改、卸载等，保证了即使服务器被非法入侵，也不能够对网站进行篡改，不能够对网站管理系统进行破坏。

（4）虚拟防火墙

虚机防火墙服务针对云数据中心与外部网络之间的南北向流量，为用户提供边界安全防护功能，支持以弹性公网IP为防护对象的入侵检测防御（IPS）和网络防病毒（AV）功能。

虚机防火墙服务的主要功能如下：

- 安全防护：可针对弹性公网IP（EIP/ELB）进行南北向流量的访问控制、入侵防御和防病毒；
- 安全日志：根据源、目的地址、日期、攻击类型、协议等查看日志明细；
- 统计报表：图表的形式展示攻击类型、趋势、协议等排行。

（5）入侵检测

数据中心环境应当提供网络入侵检测（IPS Intrusion Prevention System）：感知来自互联网以及租户虚拟网络之间东西向的攻击，并针对攻击实施检测并记录相关威胁日志，在网络边界部署了IPS&AV设备，包括但不限于外网边界、安全区域边界和租户空间边界等。IPS&AV具备网络实时流量分析能力，能防护异常协议攻击、端口/漏洞扫描、病毒/木马、针对漏洞的攻击等各种入侵行为。基于网络流量，IPS&AV可以提供信息帮助定位和调查网络异常，分配定向流量的限制策略，并采用相应的自定义检测规则，保障生产环境内的应用程序和网络基础设施安全。

（6）虚拟防病毒

可从终端视角查看所有终端病毒查杀情况，并可对所有终端批量进行病毒扫描（快速扫描/全盘扫描/自定义扫描）、停止扫描及处理病毒操作。

- 支持模板化管理信任名单。
- 支持查看单个终端的病毒查杀页面。
- 支持查杀设置，包括扫描模式（极速模式、低资源占用模式）、多引擎

设置（默认引擎、深度扫描引擎）、压缩包查杀设置、处理方式。

- 支持扫描后导出病毒查杀的结果报告。

可从病毒视角查看所有病毒威胁情况，并可单独查看病毒影响的终端、文件路径、发现时间、发现方式等信息，对病毒文件进行立即处理或删除记录。

支持病毒实时防护功能，在潜在的风险即将发生之前可介入检测，及时阻断恶意代码的运行。病毒处置时，只清除病毒、不损坏文件，基于“通用脱壳”、“行为沙盒”的纯本地反病毒引擎，无需连接外网。需支持以下场景主动防病毒能力：

- 代码执行

通常指进程启动、DLL加载、驱动加载、脚本执行时，会执行恶意代码检查，检出威胁将阻止进程执行并处置病毒。脚本类执行可覆盖无文件病毒的防御，类似PowerShell、WMI、Rundll32、Register32等。

- 文件改动

当系统中有文件变动时，也会触发恶意代码的检查，可覆盖本机文件改变，浏览器下载文件、聊天软件接收文件。并不是所有的文件变动都会引发恶意代码检查，仅针对潜在的有风险的文件，包括PE类格式（EXE、DLL、SYS等）、Linux的ELF格式、所有的文档类（可能包含宏病毒）、所有的脚本类（Web动态脚本、PS、PY、BAT、SHELL等）。

- 存储介质连接

U盘是局域网病毒传播的一种常见手段，EDR可在U盘插入电脑时感知到，并根据设置执行U盘病毒检查。

（7）虚拟 VPN 安全接入

虚拟 VPN网关为VPN隧道在VPC一端提供路由功能。虚拟VPN连接用于将VPC（Virtual Private Cloud）中的路由网络和用户所在网络通过VPN隧道连接起来，用户可以通过VPN隧道访问VPC内的业务资源。虚拟VPN安全接入需支持以下能力：

公共资源交易平台技术专用

- VPN管理

配置VPN名字，指定IP或自动方式分配VPN网关公网IP地址，配置对端地址和两端子网，配置VPN加密算法、认证算法、传输协议等

- VPN限速

对VPC通过VPN隧道访问用户自有数据中心的出口流量进行带宽控制。

- 自定义路由

VPN业务根据自定义路由转发。

- 支持国密算法和证书认证

支持《GB/T 36968-2018 信息安全技术IPSec VPN技术规范》，支持IKEv1国密证书认证，支持国家标准算法，支持证书管理。

三、审计类安全能力

（1）虚拟堡垒机

应部署堡垒机，为用户提供云主机资产的运维审计功能，堡垒机需满足以下要求：

- 产品应能覆盖 SSH、RDP、VNC、Telnet、FTP/SFTP 等多种协议；
- 应支持通过浏览器 Web 页面和本地 C/S 客户端工具的方式访问主机，从而实现事前授权、事中监察、事后审计；
- 应具备多因子鉴别功能，并确保其中一个因子由与系统分离的设备提供，以防止鉴别凭证在系统中存储时受到破坏；
- 提供多种认证方式的统一认证接口，支持与第三方认证服务器结合；
- 应提供统一的界面对用户、角色及行为和资源进行授权，达到对权限的细粒度控制；
- 应能提供自定义控制策略配置，实现细粒度的访问控制。

（2）虚拟日志审计

应部署日志审计产品，对客户网络设备、安全设备、主机和应用系统日志进行收集并分析，形成安全月报或周报，反应系统总体安全事件情况。日志审计产品应具备全面的智能收集和日志解析等功能。

公共资源交易平台投标专用

（3）虚拟数据库审计

应部署数据库审计产品，帮助用户实现对进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果。确保数据库操作的可溯源性、安全性。

数据库审计产品应满足以下要求：

- 应支持所建的多种数据库。
- 应支持事前安全风险评估、实时行为监、细粒度协议解析与双向审计、应用三层关联审计等功能。

四、数据安全类能力

（1）资产梳理

应通过工具探查、人工辅助的方式，发现和梳理数据表、数据项、数据文件等数据资产，对初始清单进行筛选优化，按照系统级、表级梳理后，对其实施价值衡量，完成资产安全性赋值，形成数据资产清单、数据权限现状和数据流向图。

（2）数据脱敏

应进行数据脱敏能力建设，灵活选择脱敏方式，满足江苏省卫生健康云影像平台存储中心开发测试、培训、离线分析等场景对敏感数据的需求，通过将敏感数据进行数据变形，提供仿真数据而非真实数据，在保证开发测试、培训、离线分析等业务需求的前提下实现敏感数据的安全，同时还应建立系统的敏感数据分布视图，提供替换、位移、哈希处理、标记化以及保留格式加密等脱敏算法，有选择性地对敏感数据进行脱敏处理，以防止敏感数据在内部使用、外部共享等环节的泄露。

（3）数据审计

应具备数据审计能力，以安全事件为中心，以全面审计和精确审计为基础，针对敏感数据的各类操作行为进行监测、记录、分析，生成审计报表。对于监测到的风险事件，及时生成告警并以邮件、短信等方式通知相关人员，确保用户的系统符合各类法律法规对数据审计的要求。审计系统的运行对数据库系统和业务操作等不应造成性能影响。

（4）数据水印溯源

公共资源交易平台投标专用

应具备数据水印技术，明确数据水印利用场景，在数据交换及数据使用中的分发共享、委托处理等环节标明数据的来源、分发对象、分发时间、分发途径及使用范围等。当出现数据泄露事件时，可从植入的数据水印信息中还原上述信息，达到追溯泄露途径、追责泄露人员的目的，避免相同类型的数据泄露事件发生。

数据水印是为版权保护和泄密溯源，将水印信息隐藏在数据库表中，当发生数据泄露时，可提取水印信息进行溯源。

（5）数据库加密服务

数据库加密服务的主要功能如下：

- 密码资源池的构建及统一调度：实现密码资源池管控系统，基于CloudHSM构建密码资源池；支持对CloudHSM、VSM自动化配置、操作、漂移、升级等；支持对密码资源池统一监管、分配、运维、告警处置等；
- 租户按需动态开通VSM：支持租户自动化开通、配置、关闭VSM资源；支持租户VSM资源总览、性能查看、VSM详情查看、组件下载等；
- VSM的安全接入租户VPC：通过网络映射，将VSM接入租户VPC，实现加密机的本地调用，保障VSM的使用、管理安全；
- 租户密码资源统一管理：支持租户统一管理名下的所有密码设备、密钥资源。

（6）虚拟密码机

CHSM 云服务器密码机 （cloud-hosted hardware security module，简称 CloudHSM 或 CHSM） ，即在云计算环境下，采用虚拟化技术，以网络形式，为多个租户的应用系统提供密码服务的密码设备。

能够为政务云提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，可以满足通用密码服务，保证传输信息的机密性、完整性和有效性，司时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。

公共资源交易平台投标专用

3.1.3.3.3 密码应用需求

3.1.3.3.3.1 通用需求

1. 密码算法

使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。基于密码算法风险，在本项目中要求按照相关政策要求，采用国家密码管理局批准的密码算法SM1/SM2/SM3/SM4。同时，要求所有硬件产品必须具有国家密码管理局的相关产品资质。

2. 密码技术

信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。作为高风险项目应避免使用存在缺陷或有安全问题警示的密码技术，如SSL1.0、SSL2.0、SSL3.0、TLS1.0、SHA-1、MD5等；杜绝使用安全性未知的密码技术，如自行设计的密码通信协议、未经安全性论证的密码通信协议等。

3. 密码产品和密码服务

信息系统中使用的密码产品、密码服务应符合法律法规的相关要求，所有产品均需具有国家密码管理局颁发的商用密码产品认证证书，所使用的第三方电子认证服务需具备工信部颁发的电子认证服务许可证、国家密码管理局颁发的电子认证服务使用密码许可证。

4. 密钥管理

平台（或系统）内使用到的对称密钥、非对称密钥（证书等）需要进行生命周期管理，覆盖密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节，保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，同时保证公钥不被非授权的修改和替换。

3.1.3.3.3.2 平台密码应用需求

1. 物理和环境安全需求分析

物理和环境安全主要实现对云平台重要场所、内部设备设施的安全防护。需要利用密码技术确保信息系统的物理和环境安全，以有效阻断外界对信息系统各类重要场所、监控设备的直接入侵，并确保监控记录信息不被恶意篡改。涉及的密码应用需求主要有：

公共资源交易平台投标专用

1）人员身份鉴别需求：保证物理和环境的访问控制真实性，基于门禁卡 + 电子门禁系统，利用商密算法实现门禁卡的“一卡一密”，对人员身份进行实体鉴别，实现未授权人员无法访问重要场所、重要设备和监控设备。

2）重要数据安全存储需求：保证各类监控信息的完整性保护，包括人员进入记录、监控记录等，对门禁进出记录和视频安防数据进行完整性保护，实现事前威慑、事中监控、事后追责。

3）三级云平台需要使用密码模块/产品达到GB/T 37092 二级（三级）及以上安全要求。

2. 网络和通信安全需求分析

网络和通信安全主要实现对云平台与经由外部网络连接的实体、内部跨物理机房通信时进行网络通信安全防护，涉及的密码应用需求主要有：

1）身份鉴别需求：云平台与网络边界外进行远程通信时，应采用密码技术，实现进行通信实体的身份标识和双向身份鉴别，保证通信实体身份的真实性。

2）重要数据传输安全：云平台与网络边界外、内部跨物理机房进行远程通信过程中，应采用加密措施，防止重要数据被非法获取；云平台与网络边界外进行远程通信过程中应实现对访问控制信息的完整性保护，防止重要数据被非法篡改；需部署商密IPSec VPN、商密SSL VPN、安全认证网关等设备，配合商密浏览器和智能密码钥匙，实现商密https协议构建，搭建商密SSL加密通道，实现通信双方加密通信，满足通信过程中保证重要数据在的完整性和机密性需求，满足通信双方身份鉴别需求。

3）网络边界访问控制信息安全需求：云平台与网络边界外进行远程通信时应实现对访问控制信息的完整性保护，防止云平台网络边界、网络区域边界、虚拟化网络边界的访问控制信息被非法篡改；需通过IPSec VPN、SSL VPN、安全认证网关等设备基于完整性校验，对网络边界访问控制信息、系统资源访问控制信息进行完整性保护（潜在需要设备支持）。

4）三级云平台需要使用密码模块/产品达到GB/T 37092 二级（三级）及以上安全要求。

3. 设备和计算安全需求分析

设备和计算安全主要实现对云平台中物理机、虚拟机等安全防护，为云平台自身以及云上业务应用系统所涉及的各类设备提供密码支撑和保障作用，涉及的密码应用需求主要有：

1）身份鉴别需求：对于登录各类物理及虚拟设备的云平台管理用户、云租户管理用户，应进行身份标识和鉴别，保证云平台管理员、云租户管理员的真实性。由于Host OS、GuesOS等由开源Linux、闭源Windows等为主，OS改造有所限制，可先在堡垒机登录认证，基于用户名/口令及智能密码钥匙等认证成功后，再接入设备。

2）安全管理通道需求：远程管理云平台中各类物理及虚拟设备时，应基于SSH等建立安全的信息传输通道，实现身份鉴别信息的防截获、防假冒和防重用。如OS无法支持SSH等改造时，可在设备前部署支持商密的SSL协议堡垒机，实现管理过程中通信的机密性、完整性。

3）重要数据完整性需求：各类物理、虚拟设备等系统资源的访问控制信息、重要信息资源安全标记、日志记录等，在OS存储过程中应基于AIDE、IMA等机制，结合HMAC或数字签名等密码技术实现完整性保护，防止重要资源数据被恶意篡改。

4）可执行程序完整性需求：对于云平台中各类设备上的重要可执行程序（如镜像等），应实现完整性保护，验证其来源的真实性，防止重要可执行程序被非法篡改后运行在云平台内部设备上。

5）三级云平台需要使用密码模块/产品达到GB/T 37092 二级（三级）及以上安全要求。

4. 应用和数据安全需求分析

云平台可以视作一个包含上百个微服务的复杂应用，应用和数据安全是云平台安全防护的核心，涉及的密码应用需求主要有：

1)身份鉴别需求：对于访问云管系统、服务 Console 等的云平台管理员、云租户管理员，应进行身份标识和鉴别，保证云平台管理员、云租户管理员身份的真实性。云平台系统用户配置基于数字证书的智能密码钥匙（证书可与用户身份绑定），实现用户登录系统的身份鉴别。

2)访问控制信息完整性需求：云管、云服务 IAM 等自身利用物理密码机或密码模块，采用 HMAC-SM3 对其访问控制策略、数据库表访问控制信息进行完整性保护。

3）重要数据安全存储需求：云平台各服务内部身份鉴别信息、云租户信息、敏感数据等重要数据在存储过程中，应采取加密措施，防止重要数据被非法获取；身份鉴别信息、操作日志、虚拟机镜像文件等重要数据在存储过程中应实现完整性保护，防止重要数据被恶意篡改。

4） 重要数据安全传输需求：身份鉴别信息、云租户敏感信息等重要数据在传输过程中，应采取加密措施，防止重要数据被非法获取；身份鉴别信息、云资源管理信息、操作日志、告警、虚拟机镜像文件等重要数据在传输过程中应实现完整性保护，防止重要数据被恶意篡改。

5） 关键操作不可否认性需求：对于涉及法律责任认定的应用，对关键操作应提供数据原发证据和数据接收证据，实现相关行为的不可否认性。

6）三级云平台需要使用密码模块/产品达到 GB/T 37092 二级（三级）及以上安全要求。

5. 密钥管理需求分析

云平台内使用到的对称密钥、非对称密钥（证书等）需要进行生命周期管理，覆盖密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节，保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，同时保证公钥不被非授权的修改和替换。

6. 安全管理需求分析

需要依据《GB/T 39786-2021 信息系统密码应用基本要求》，从信息系统的管理制度、人员管理、建设运行、应急处置四个方面制定密码应用管理要求，为信息系统提供管理方面的密码应用安全保障。

3.1.3.3.3.3 租户密码应用需求

按照信息系统密码应用基本要求，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理等层面，对存在的安全风险采用有效的技术手段进行防护，确保租户应用系统的安全。

1. 物理和环境安全需求分析

按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中的第三级信息系统密码应用要求，租户应用系统的物理和环境安全需求描述如下：

（1） 宜采用满足《GM/T 0036-2014 采用非接触卡的门禁系统密码应用指南》要求的电子门禁系统，对重要区域进入人员的身份进行鉴别。

（2）宜采用密码技术来保证电子门禁系统进出记录和视频监控音像记录的存储完整性，防止记录数据被篡改。

2. 网络和通信安全需求分析

按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中的第三级信息系统密码应用要求，租户应用系统的网络和通信安全需求描述如下：

（1）应采用密码技术对通信实体的身份进行认证，防止身份信息被假冒和重用，确保通信实体身份的真实性。

（2）宜采用密码技术保证网络边界访问控制信息的完整性，防止访问控制信息被篡改。

（3）应/宜采用密码技术保证通信过程中数据的机密性/完整性，防止通信数据在网络传输过程中被窃听和篡改。

3. 设备和计算安全需求分析

按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中的第三级信息系统密码应用要求，租户应用系统的设备和计算安全需求描述如下：

（1）管理员登录设备前应采用密码技术对其身份进行认证，防止身份信息被假冒和重用，确保登录人员身份的真实性。

（2）设备管理员在远程管理设备前，应采用密码技术建立安全的信息传输通道，防止管理数据在传输过程中被非法获取和篡改。

（3）宜采用密码技术保证系统资源访问控制信息、设备种的重要信息资源安全标记和日志记录的完整性，防止重要信息和记录被篡改。

（4）宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。

4. 应用和数据安全需求分析

按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中的第三级信息系统密码应用要求，租户应用系统的应用和数据安全需求描述如下：

公共资源交易平台技标专用

（1）用户在登录应用系统前，应采用密码技术对登录人员的身份进行认证，确保应用系统访问人员身份的真实性。

（2）宜采用密码技术保证信息系统应用的访问控制信息和重要信息资源安全标记的完整性，防止访问控制信息和安全标记被篡改。

（3）信息系统应用的重要数据在传输和存储的过程中应采用密码技术对其进行机密性保护，防止重要数据的泄露。

（4）信息系统应用的重要数据在传输和存储的过程中宜采用密码技术对其进行完整性保护，防止重要数据被篡改。

（5）在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，确保数据发送行为和数据接收行为的不可否认性.

3.1.4 建设内容及标准

根据南阳市政府关于政务云平台建设的相关要求，南阳市政务服务和大数据管理局组织进行政务云服务采购。政务云主要为全市各政务部门提供高性能物理机、云主机、云存储、云应用、云安全和异地备份等基础设施资源共享服务，为各政务部门间数据交换、共享、应用等提供基础平台支撑。本项目服务对象是党政机关、事业单位等。

服务建设内容包括计算资源、操作系统、存储、数据备份、负载均衡、云数据库、大数据服务、容器服务、应用服务、网络及托管服务、云桌面等；

租户安全服务包括虚拟防火墙、虚拟漏洞扫描、虚拟堡垒机、虚拟主机安全、虚拟 Web 应用防火墙、网页防篡改、虚拟日志审计、虚拟 VPN 安全接入、虚拟防病毒、入侵检测、虚拟数据库审计、虚拟密码机、数据库加密服务等。

3.1.4.1 技术要求

本技术要求参照《关于发布<国家电子政务外网信息安全标准体系框架> 等七项安全标准的通知》（政务外网〔2014〕11 号）、《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55 号）、《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》（国办函〔2016〕108 号）等文件制定。

本技术要求是基本要求，投标人可进行优化，具体响应方案中的功能性能可优于本技术要求。

公共资源交易平台 投标专用

（1）投标人须承诺配合采购人做好政务云监管平台接入及政务云安全工作，确保本项目达到国家监管部门要求。

（2）投标人承诺在签订合同后按工期完成云服务平台安装部署，并具备服务能力。

（3）投标人须承诺无条件做好各单位业务应用迁移上云工作。

（4）投标人须承诺未经允许不得对云平台上的任何数据进行截取、加工、分析和处理，或提供给第三方。

（5）投标人须承诺在服务期结束后，无条件配合各使用单位迁移应用系统，提供服务退出承诺书。

（6）机房要求：提供云平台需要的机房环境，包含安全可控的独立机房区域、电力、机柜、制冷、门禁及视频监控等，标准不低于国标 B 级。

（7）云管理平台要求：通过云管理平台软件对资源进行管理，提供弹性计算、自动化部署、资源区域划分等功能，通过统一的接口为云运营平台和云监管平台提供相关功能要求。

（9）基础安全要求：符合《信息安全技术 云计算服务安全指南》(GB/T31167-2014)、《信息安全技术 网络安全等级保护实施指南》(GB/T25058-2019)、《信息系统密码应用基本要求》(GM/T0054-2018)等规范要求，政务云平台应通过信息安全等级保护三级认证、商用密码应用安全性评估、云计算服务安全评估。政务云平台应在不同层面保障政务云安全，包括基础设施安全、云平台安全、云租户安全、平台运维安全、平台合规审计等，并提供网络隔离、租户隔离、漏洞扫描、主机安全、日志审计、通用密码、数据库加密等安全及密码能力。

采购的云计算服务，相关网络安全部分，如果未有明确要求，按上级政策规定执行。

（10）网络要求：提供 SDN、VxLAN 相关网络服务，支持与互联网、电子政务外网及行业部门专网的连接。提供与电子政务外网核心交换节点连接的专线。

（11）投标人必须按照采购人要求，提供详细的技术实施方案。

（12）配合各政务部门使用政务云或者迁移应用系统至政务云平台等相关工作，投标人主要负责但不限于如下工作：

1）配合各单位应用系统迁移前的环境需求分析工作。

2）负责各单位应用系统迁移前的测试环境搭建工作。

公共资源交易平台投标专用

3）配置物理服务器、配置虚拟机、配置网络、安装操作系统、配置相应的安全策略等。

4）配合或提供各单位应用系统迁移需要使用的迁移工具。

5）配合各单位应用系统迁移过程中遇到问题故障分析以及提出解决方案，并配合解决问题故障。

6）负责各单位应用系统迁移过程中对硬件、网络、软件、安全等运行环境的变更工作。

7）配合各单位应用系统迁移后进行测试工作，如压力测试、故障测试等。

3.1.4.2 **服务要求**

1、技术要求概览：

序号	服务名称	服务要求
1	机房	机房空间要求满足本期摆放空间，并具备后期扩展能力
2	传输线路	提供 2 路及以上传输线路
3	云管理平台	提供云服务器生命周期管理包括镜像与磁盘管理、安全组，提供云平台操作截图证明。 提供云服务器 CPU 和内存状态监控功能，监控内容包括不限于 24 小时的 CPU 利用率趋势图、内存使用率趋势，提供云平台操作截图证明；提供云服务器网络监控功能，监控内容包括网络流入带宽、网络流出带宽，提供云平台操作截图证明； 所使用的云平台支持云服务器快照功能，提供云平台操作截图证明。 所使用的云平台支持短信、邮件告警通知，提供云平台操作截图证明。
4	计算资源池	云主机（ECS）可用性≥99.99%，提供相关证明材料。
5	存储资源池	块存储（云硬盘）和对象存储数据存储持久性≥ 99.9999%，提供提供相关证明材料。
6	网络资源池	提供满足要求的网络资源池能力
7	安全资源池	提供满足要求的虚拟化安全能力

公共资源交易平台 投标专用

8	云数据库	云数据库业务可用性满足基本要求且≥99.99%，云数据库的数据存储持久性≥99.9999%,提供相关证明材料。
9	监管接口	提供满足云监管平台和统一安全运维所需的接口
10	运维要求	提供满足政务云标准要求的运维服务方案
11	故障处理	提供满足政务云标准要求的故障处理方案
12	应急响应	提供满足政务云标准要求的应急响应方案
13	信息安全保障服务	提供满足政务云标准要求的信息安全保障服务方案
14	租户安全	安全部分应满足租户安全需要，保证政务业务系统的网络安全、数据安全等。

2、运维要求：

投标人需提供素质高、专业性强、经验丰富、稳定的运维团队，主要负责整个政务云平台的软硬件和网络运维。投标人需要为本项目选派专业技术人员参与本项目实施运维，需运维人员至少 8 名，包括云核心技术提供方的原厂或原厂授权运维人员至少 3 名、其他运维人员至少 5 名。投标人需有严格的、有组织、有纪律的管理运维流程，并指派专职联络员，团队需要 7×24 小时在岗及时响应故障请求，负责云平台的故障受理、处理、跟踪、结果汇报工作。

为保证云平台服务可用性及运行效率，供应商云平台的服务能力须保证各个应用系统可用性不低于 99.99%；供应商云资源交付响应时间不超过 2 个工作日。

运维方案应从整运维服务体系的宗旨、运维服务体系架构、运维服务体系的内容、运维管理制度、人员培训等方面来阐述说明。

3、故障处理

投标人必须承诺在签订合同后，实行 7×24 小时运行维护和响应故障工作，负责政务云平台的故障受理、处理、跟踪、结果汇报工作。切实保障政务云平台基础环境的安全、稳定、高效的运行。

对于一般故障要求投标人 30 分钟内进行响应；对于重大故障要求 10 分钟内进行响应；对于特别重大故障要求 5 分钟内进行响应。

公共资源交易平台投标专用
AE2C1CCE27C4B1A624B1C88EA1DB9

故障处理方案应从故障处理的流程、网络故障处理、服务器故障处理、业务系统故障处理等方面来阐述说明。

4、应急响应

投标人应提供系统故障应急处理预案，提供出现问题的快速解决方法，制定完善合理的应急响应方案。

投标人每年应进行不少于 2 次的应急演练。

应急响应方案应从响应时间、电力应急、空调应急、消防应急、网络及系统应急、云平台故障应急等方面来阐述说明。

5、信息安全保障服务

投标人应遵循国家电子政务信息安全保障体系要求，参考国家主管部门发布的相关标准规范要求，提供明确、完善、可行的安全建设方案，充分考虑在网络、系统、数据库、应用等方面的安全性。

投标人须从机房、网络、安全、虚拟机、物理机、存储、运维等方面加强信息安全管理，避免因出现问题引起信息安全责任事故。

信息安全保障服务方案应从保障措施、预防措施、风险评估、质量保障等方面来阐述说明。

3.1.5 建设依据

政务云建设方案参考如下相关政策发文与标准规范：

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27 号）；

《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号）；

《国家电子政务总体框架》（国信[2006]2 号）

《信息安全等级保护管理办法》（公通字〔2007〕43 号）

《关于开展信息安全等级保护安全建设整改工作的指导意见》公信安〔2009〕1429 号

《信息系统等级保护安全设计技术要求》（信安秘字〔2009〕059）

《国家电子政务“十二五”规划》（工信部规〔2011〕567 号）

《国务院关于促进信息消费扩大内需的若干意见》（国发〔2013〕32 号）

《智慧城市公共信息平台建设指南(试行)》（住建部〔2013〕）

公共资源交易平台投标专用

《基于云计算的电子政务公共平台顶层设计指南》（工信信函〔2013〕2 号）

《关于进一步加强政务部门信息共享建设管理的指导意见》（发改高技〔2013〕733 号）

《国家新型城镇化规划(2014-2020 年)》

《国务院关于促进云计算创新发展培育信息产业新业态的意见》（[2015]5 号）

《国务院关于印发促进大数据发展行动纲要的通知》国发〔2015〕50 号

《国家发展改革委办公厅关于组织实施促进大数据发展重大工程的通知》发改办高技〔2016〕42 号

《推进“互联网+政务服务”开展信息惠民试点实施方案》（国办发〔2016〕23 号）

《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55 号）

《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》（国办函〔2016〕108 号）

《关于开展信息惠民国家试点城市 2016 年建设成效评价工作的通知》（国家发改委〔2016〕1339 号）

《河南省政务信息系统整合共享实施方案》豫政办〔2017〕116 号

《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）

《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》（国办函〔2022〕102 号）

《河南省加强数字政府建设实施方案（2023—2025 年）》（豫政〔2023〕17 号）

《南阳市新型智慧城市和数字政府建设总体规划(2022—2025 年)》（宛政办〔2022〕4 号）

《南阳市数字政府建设实施方案(2022-2025)》 宛政办〔2022〕50 号

《统筹推进数字政府和新型智慧城市建设的若干意见》（宛办〔2023〕7 号）

《电子政务信息共享互联互通平台总体框架技术指南》

《国家电子政务工程建设项目管理暂行办法》

《“十四五”国家信息化规划》

《国家智慧城市试点暂行管理办法》

公共资源交易平台投标专用

《国家智慧城市（区、镇）试点指标体系（试行）》

《基于云计算的电子政务公共平台顶层设计指南》（工业和信息化部）

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

《政务信息资源交换体系标准》（GB/T 21062-2007）

《政务信息资源目录体系标准》（GB/T 21063-2007）

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息系统安全等级保护基本要求》（GB/T22239-2008）

《河南省网络与信息安全综合管控平台建设指南》

3.2 政务云部署方案

3.2.1 政务云机房建设方案

3.2.1.1 数据中心机房整体介绍

南阳移动立足“满足现在、适应未来”的建设策略，已建成符合政务云数据中心标准的现代化机房，具备承载本期政务云服务项目的条件。政务云数据中心机房位于将南阳张衡路移动 IDC 枢纽楼，为政务云平台划分独立机房区域。

数据中心位于南阳市中心城区，位置如下图所示：



政务云数据中心位于张衡东路，距白河约 1.5 公里，不在洪水威胁范围之内，历史上也没有发生过洪水。政务云数据中心位于南阳移动的枢纽楼，整栋枢纽楼按照中国移动高标准机房进行建设，没有其他租户，非常安全，适宜作为政务云数据中心。

公共资源交易平台投标专用

政务云数据中心机房符合国际 T3 标准，机房面积 800 平米，具有抗 8 级地震能力，双重电源供电，独立于正常电源的双路柴油发电机组和完善配套设施，满足国家信息安全等级保护三级要求。

政务云数据中心充分依托河南移动资源平台，机房内带宽充裕，物理线路出口从 3 个单独的路由方向接入机房，直通河南移动骨干网。全面领先南阳，全冗余网络结构，杜绝单点故障，千兆级带宽，突破网络瓶颈。

3.2.1.2 机房设计标准

南阳市政务云数据中心机房解决方案参考了大量的国家标准(GB)和电信企业标准，从而有效避免了可能出现的机房建设及运行风险。

（1）《工业企业厂界环境噪声排放标准》（GB 12348-2008）；

（2）《建筑设计防火规范》（GB 50016-2014（2018 版））；

（3）《通信局（站）防雷与接地工程设计规范》（GB 50689-2011）；

（4）《通信工程建设环境保护技术暂行规定》（YD 5039-2009）；

（5）《通信建筑抗震设防分类标准》（YD 5054-2010）；

（6）《电信设备安装抗震设计规范》（YD 5059-2005）；

（7）《通信工程设计文件编制规定》（YD/T 5211-2014）；

（8）《通信设备安装抗震设计图集》（YD 5060-2010）；

（9）《通信局（站）节能设计规范》（YD 5184-2009）；

（10）《通信建设工程安全生产操作规范》（YD 5201-2014）；

（11）《通信中心机房环境条件要求》（YD/T 1821-2008）；

（12）《通信机房安全管理总体要求》（YD/T 2057-2009）；

（13）《通信电源设备安装工程验收规范》（YD 5079-2005）；

（14）《通信建设工程节能与环境保护监理暂行规定》（YD 5205-2014 ；

（15）《建筑施工场界环境噪声排放标准》（GB 12523-2011）；

（16）《数据中心设计规范》（GB 50174-2017）；

（17）《数据中心基础设施施工及验收规范》（GB 50462-2015）；

（18）《建筑物电子信息系统防雷技术规范》（GB 50343-2012）；

（19）《电磁环境控制限值》（GB 8702-2014）；

公共资源交易平台投标专用

（20）《通信建筑工程设计规范》（YD 5003-2014）；

（21）《通信局（站）防雷与接地工程设计规范》（YD 5098-2005）；

（22）《通信机房防火封堵安全技术要求》（YD/T 2199-2010）；

（23）中国移动通信集团《中国移动通信防火封堵管理规定》；

（24）《关于中国移动 IDC 建设工作的指导意见》；

（25）《中国移动 IDC 业务规范》；

（26）中国移动通信集团下发的《中国移动 IDC 总体技术要求》；

（27）中国移动通信集团下发的《中国移动 IDC 设备规范》；

（28）中国移动通信集团下发的《中国移动 IDC 机房规范》；

（29）中国移动 IDC/ISP 信息安全管理系统总体技术要求；

（30）中国移动 IDC/ISP 信息安全管理系统控制平台设备规范；

（31） 中国移动通信集团《中国移动通信集团通信机房配套标准化建设指导意见》；

3.2.1.3 **电力保障**

南阳市政务云机房大楼供电标准按照集团公司最新设计理念进行设计建设，综合考虑安全、节能、稳定、冗余等诸多因素，达到 Tier3 级机房的标准要求。南阳市政务云数据中心采用两路市电，两路高压分别从两个变电站专线引入，可互为备用也可分带业务，高低压配电采用集中供电方式，按照大楼用电终期容量设计安装 ，各系统均考虑有备份。共安装 1600KVA 变压器 4 台，采用 3+1 供电保障方式，1 台备用变压器可以为其他 3 台主用变压器的任一台互为备用，满足 IDC 机房具有 2 路 10KV 高压电力专线从不同变压器接入的要求；并安装 1800KW 备用柴油发电机两台，发电机互为备用也可并机使用，可满足大楼全部用电设备的应急供电保障，为符合环保要求，油机室专门做了降噪处理，油机噪声符合环保要求。

电力机房主要负责政务云数据中心的供电，共安装艾默生组合开关电源 4 套，3000AH 蓄电池 8 组，主要为 48V 直流系统提供供电保障，市电停电情况下，可以提供 10 小时不间断供电保障；安装 200KVA 不间断交流供电系统两套，两套系统都是 1+1 并机系统 ，两套系统互为备份，确保单套系统故障或检修时不间断

公共资源交易平台投标专用

供电，该系统可以在市电停电情况下提供 3 个小时不间断交流供电。

3.2.1.4 空调系统设计

政务云数据中心部署机房精密空调 6 台，采用 5+1 冗余备份的方式，可以为政务云机房提供 500 千瓦的制冷量，能够保证数据中心恒温恒湿，夏季温度 23±2℃，冬季温度 20±2℃，相对湿度保持在 45%~65%温度变化率：<5℃/h，不结露。防尘：静态条件下测试，空气中≥0.5μm 的尘粒数，少于 18000 粒/升。有专业空调维护队伍；对机房温湿度有监控措施和记录。



政务云数据中心采用地板下送风、顶回风的空调形式，将低温空气直接从底部送到机柜内，吸收机柜的热量后，从机房顶部回到精密空调顶部，该气流组织方式具有以下优点：

1、空调风流动方向与空气特性相一致，容易得到好的空调效果。

2、地板下的空间比风管断面的面积要大许多，这就形成了静压箱，因此下送风方式送风均匀，整个机房区域的温差小。

3、因为送风是在活动地板内，从而使下风的距离与上送风方式在同等条件下，所需的送风风压低，精密空调的送风噪声相对会低一些。

公共资源交易平台投标专用
A1C7646E1A62A8BC88EA14DB9

4、单从空调专业的角度出发，下送风方式不需送风风管和送风口，对于设计施工来说，相对简单方便。精密空调设备的摆放就可以灵活的进行调整。

5、由于下送风将通信工艺所需的各类管线，空调专业的管线均隐藏在活动地板内，从而使得通信机房内显得整齐美观。



活动地板下送风示意图

电力电池室采用风管上送风、侧回风的空调形式，将多台精密空调的低温空气向上均匀的送到电源室各处，吸收热量后，再通过精密空调正面回风，该气流组织方式具有以下优点：

1、容易实现备份冗余，精密空调中有一台停机后，剩余精密空调的冷量仍可以送到电源室的每个区域。

2、机房内没有活动地板，不易积灰，即使房间有灰尘，清理打扫很方便，从而使精密空调的过滤网使用时间长，减少维护管理的工作量。

3.2.1.5 **消防系统设计**

政务云数据中心消防系统包含消防报警系统及自动灭火系统两部分。其中消防报警系统采用早期烟雾报警系统，及时侦测火灾隐患，赢得处理时间，降低火灾危害；自动灭火系统采用气体灭火系统对数据中心进行灭火。

从功能结构上，本项目消防系统主要涉及消防报警系统及手动自动灭火系统两部分，各子系统主要包括：

早期烟雾报警系统：在云数据中心设置感烟探测器、感温探测器，并接入火灾自动报警系统。

气体灭火系统：云数据中心机房，电力电池室

政务云数据中心所有功能间区域设置离子型感烟探测器和感温探测器，配置壁挂式扬声器和吸顶式扬声器用于消防广播，所有设备都要接入火灾自动报警系统。系统如下所示：



政务云数据中心采用全淹没灭火方案，气体灭火剂采用七氟丙烷。

七氟丙烷，常温下气态，无色、无臭、不导电、无腐蚀，无环保限制，大气存留期较短，当七氟丙烷灭火气体应用于全淹没式的系统环境时，它能够结合物理的和化学的反应过程迅速，有效地消除热能，阻止火灾的发生，七氟丙烷的物理特性表现在其分子汽化阶段能迅速冷却火焰温度；并且在化学反应过程中释放游离基，能最终阻止燃烧的连锁反应。这对抢救性保护精密电子设备及贵重物品是有利的。七氟丙烷洁净气体灭火剂对环境无害，在自然中的存留期短，灭火效率高并无毒适用于有工作人员常驻的保护区。

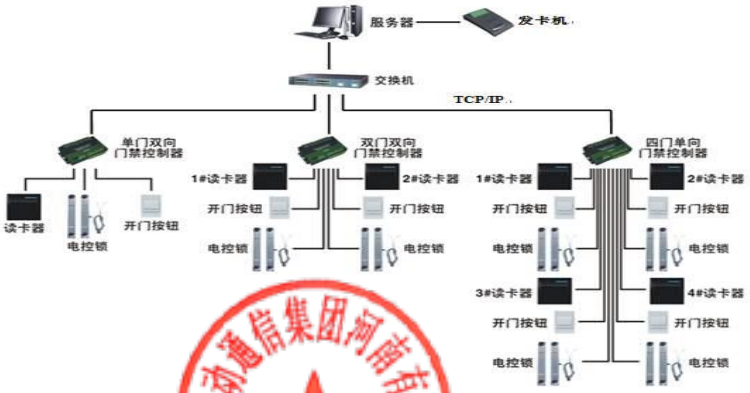
3.2.1.6 机房安防设计

政务云数据中心的安全是重中之重，我方采取 7*24 小时保安值班，严格的安全检查与身份认证，各机房出入口及周边均配置门禁及视频监控系统，配置防尾随门禁闸道，严格控制进入人员，机房内各区间无死角视频监控录像。

门禁系统

对机房内各主要进出通道实施门禁进出管理，实时对各指纹识别读卡器所读到的数据记录并显示在门禁管理资料中，并可通过门磁实时监视各门的开关状态。门禁系统通过门禁控制器接入到机房管理系统进行管理。

政务云数据中心采用单向感应模式，读卡器能同时支持单独卡，单独指纹，卡+指纹三种不同的验证方式。



门禁系统由电源、读卡器、控制器、电锁（带门磁）、出门按钮、机箱、感应卡、门禁软件等组成：

- 单向感应模式
- 单向感应模式在进方向配置 1 个读卡器、出方向配置出门按钮。
- 双向感应模式
- 双向感应模式则在进、出方向各配置 1 个读卡器。
- 读卡器能同时支持单独卡，单独指纹，卡+指纹三种不同的验证方式。

视频监控系统

政务云数据中心在公共区域和出入口处、机房内机架间、核心机房、控制中心、动力机房,楼梯与走廊,楼梯等均装有摄象机，对机房内的各个人员出入点和重要设备区域进行实时监测，实现对机房内各区间无死角视频监控录像。

政务云数据中心中采用数字视频监控系统,实时显示视频并保存历史记录 30 天，图像清晰，同时能对历史视频进行回放，视频监控系统通过交换机接入到机房管理进行统一管理。



公共资源交易平台投标专用

视频监控系统由摄像机部分、传输部分、存储部分以及显示部分四大块组成。集视频监控、图像存储、数据管理、模拟接入等功能于一身，提供集成一体化视频监控核心；基于 NVR 构架的视频存储节约了存储服务器的成本，可轻松实现视频监控云存储。

同时对政务云数据中心，还配备安保人员，7*24 小时保安值班，严格的安全检查与身份认证。

3.2.1.7 **机房运维保障方案**

政务云数据中心拥有良好的运维保障方案，对机房实现 7*24 小时的监控和值守，保证机房的安全稳定运行，电信级智能网络运行监控平台，实时监控运行状态，专门配属具备多年大型 IDC 维护经验，资深电力、空调等动力设施维护支持人员和资深网络等基础设施运维人员。

政务云数据中心部署动力与环境监控系统，对数据中心的动力、空调、环境量（温湿度、水浸）等设备进行监控，监控对象如下：

序号	系统名称	监控范围
1	空调设备监测	在电力室安装的房间级空调； 在机房安装的 6 台房间级空调；
2	UPS 监测	在电力室安装 4 台 UPS；
3	配电柜监测	在电力室安装的 UPS 输入输出柜，空调配电柜； 在机房安装的空调配电柜；
4	列头柜监测	在机房内安装的列头柜；
5	温湿度监测	在电力室安装的温湿度传感器； 在机房内安装的温湿度传感器；
6	水浸报警监测	在电力室安装的漏水传感器； 在机房内安装的漏水传感器；

此外，对于政务云数据中心建立了专门的运维团队，配备资深的电力、空调等动力设施维护支持人员和资深网络等基础设施运维人员，人员具备多年大型 IDC 维护经验。运维队伍对整个数据中心进行 7*24 小时的监控，及时发现运行异常并进行处理，同时还对设备进行定期巡检，保证了政务云数据中心正常运行。

公共资源交易平台 技标专用

3.2.2 传输建设方案

我方按照国家电子政务外网相关规范，采取严格的安全措施，实现与南阳市电子政务外网的公共服务区和互联网应用区有效对接，实现各种业务和数据的完全互联互通，通过技术手段实现南阳市智慧城市云数据中心与本次采购内容的互联互通和资源共享，提供 2 条 20G 及以上速率的裸光纤政务网络接入服务能力。

专线开通时限：指采购人各入网单位填写业务受理单之日起，至为用户开通专线接入服务（不包括用户设备）实际占用的时间；最长为 30 日。

专线开通标志：两端线路均按要求到达用户指定位置，采购人两端入网单位签字认可后，即视为开通。如遇特殊情况，双方可进行具体协商。

提供的服务具体标准满足工信部颁布的《电信服务规范》，保证使用通信业务安全畅通。网络可用率≥99.9%；主干环路切换时间＜50ms；端到端电路（采购人中心节点到各分支节点）的传输比特差错率（误码率）≤1.0×10E-7；全网中断次数≤20 次/年；单点中断次数≤5 次/年。故障响应时间小于 10 分钟，故障响应率达到 100%，业务恢复时限小于 4 小时（由于光缆中断、甲方原因、不可抗力、正常割接导致的专线中断除外）。

根据《工业和信息化部关于进一步落实网站备案信息真实性核验工作方案（ 试行 ）》、工业和信息化部《关于进一步加强网站备案管理工作的通知》等文件的要求，如有网站接入，需提供网站备案相关的文件，供应商需提供在工信部的网站备案服务，备案完成后及时完成业务开通服务和开放互联网站访问服务。

3.2.2.1 传输网络简介

河南移动在南阳公下辖 14 个分公司，网络覆盖全市 14 个县/市区、所有乡镇、主要旅游景点和交通干线。全市市区室外覆盖为 99.9%，室内覆盖也达到了 99. 8%，乡村覆盖率为 99%，其中自然村的覆盖率也达到 98%。

目前河南移动南阳公司组建的基础专线网络（市、县、乡三级骨干）均已安装到位，并在线运行，完全能够满足南阳市平安城市网络系统建设的工作目标。

3.2.2.1.1 干线传输网现状

河南移动南阳公司干线传输网采用 DWDM+SDH 的方式进行组网，具有容量大、组网方便、网络安全可靠、集中统一监控等特点。全网采用二纤复用段保护环的方式进行网络架设，对所有业务进行 100％的全保护，网络具有非常高的安全性。

网络设备可提供的包括 2M、10M、100M、155M、622M、GE、2.5G、10G 等速率传输通道。

3.2.2.1.2 本地传输网现状

河南移动南阳公司经过多年建设，已形成一个由骨干传送层、汇聚传送层及接入传送层组成的城域传输网，网络已覆盖到各市（县）乡镇一级。

在网络结构上，主干传送层、汇聚传送层采用环型网络结构，并且两层面之间通过双节点互联；在接入层根据传输节点的自然地理位置及公路走向，结合城域传送网的路由情况，以环网结构组网，提供具有保护的传输通道，各业务 100%全保护，网上可提供的包括 2M、10M、100M，155M、1000M、GE 等级别的各种传输通道。

在光缆建设方面，城区主要干道均采用管道敷设，城外采用架空敷设方式为主，特殊地段部分采用了直埋敷设方式，所有光缆均为 G.652 光缆。

3.2.2.1.3 传输网应用优势

河南移动南阳公司传输网由干线传输网和本地传输网组成，现已覆盖所有县/市区，通达所有乡镇。实现各种业务的高速、全程接入，在数据业务接入方面具有许多特点与优势。

覆盖范围广

河南移动南阳公司的基站遍及市内各个角落，有河南移动南阳公司基站的地方就有河南移动南阳公司的传输网络，河南移动南阳公司的传输网络具有广阔的传输资源。

传输速率高

市干线采用的是在 DWDM 平台建设 SDH+PTN+GPON 的系统方式，具有传输容量大、扩容方便、易于维护等特点，全面为用户提供从 2M 到 GE 级别的传输通道。

接入业务丰富

河南移动南阳公司传输网现承载着 GSM 语音、GSM 信令、CMNET、GPRS、集团客户数据业务、DCN、WLAN、彩铃、客服、短信、彩信、机房集中监控、视频会议系统、企业 BOSS 系统等各类业务。

网络安全可靠

河南移动南阳公司传输网无论是干线还是本地网采用的都是环状组网的组

公共资源交易平台技术专用

织方式，对所有业务进行 100％全保护，任何故障倒换时间都在 50ms 以内，并且全网各地市按双节点双平面的结构进行系统组织，任何一个节点出现故障都不至使该地市传输业务被全部阻断，使全网安全性得到进一步提高。

同时具有有线接入和无线接入的能力

河南移动南阳公司除拥有高速光纤传输网络之外，还拥有南阳最大的无线通信网络，可以发挥两种接入方式各自的优势，相互补充。河南移动南阳公司不仅拥有丰富的传输资源，同时更是全市最大的移动业务运营商，拥有 GPRS/EDGE/TD-SCDMA/WLAN 等无线宽带接入能力。

3.2.2.2 CMNET网络介绍

CMNET 是河南移动运营管理的互联网，它除了为用户提供传统的互联网业务，还承载着与移动通信有关各类数据业务，如 WAP、GPRS、彩信和梦网短信等。

河南移动南阳公司 CMNET 经过三期工程的建设，目前已建成覆盖全市 14 各县/市区的综合业务承载网络。河南移动 CMNET 从网络结构和管理角度上可分为国家骨干网、省网、IP 城域网三层。省网分为骨干层、汇聚层和接入层。城域网分为骨干层、汇聚层和接入层。

河南移动南阳公司 CMNET 的基本建网特点是大容量、广覆盖和轻载运行。河南移动南阳公司 CMNET 网络全网采用快速路由收敛技术，以硬件线速转发方式支持 IPV4/IPv6，QoS 服务、组播、MPLS VPN、协议平滑重启等功能，同时全网采用开放的业务策略，能够快速支撑增值业务的开展。 河南移动南阳公司 CMNET 网络在物理拓扑设计上，采用了集中化的策略。在保持网络层次化的同时，尽量简化网络结构，采取了城域为核心集中汇聚的方式，减少了端到端的路由跳数，保证网络的性能和可管理性。河南移动南阳公司 CMNET 网络在路由设计上采用扁平化思路。城域网 IGP 协议采用成熟的 OSPF 协议，所有城域网路由器在同一 OSPF 骨干区域内，充分利用等价路径负载分担技术，按照全市城域网单平面设计路由。市骨干层 IGP 协议采用高效的 IS-IS 协议。BGP 采用 BGP-4 协议和一级路由反射器(RR)结构实现 IBGP 和 EBGP 在等价路径情况下的负载分担，实现 IGP 和 BGP 的完美配合。

河南移动南阳公司 CMNET 网络的核心技术是 IP/MPLS。在 IP 层面，实现快速路由收敛、等价路径负载分担、IGP/BGP 的协议平滑重启、组播，并具备全

网平滑升级到 IPv6 的能力；河南移动南阳公司 CMNET 网络采用轻载方式、全网具备快速部署 QoS 策略能力；在 MPLS 层面，核心节点之间采用多链路负载方式，实现故障的快速保护切换；河南移动南阳公司 CMNET 网络可以提供全网 MPLS VPN 业务；在所有接入链路端口上具备部署反向转发查找(uRPF)和安全控制列表(ACL)等安全控制功能。

河南移动南阳公司 CMNET 网络配套建设了专业的网络管理系统，采用全网集中管理的思路，重点强化了 VPN 业务管理、业务流量管理、网络故障管理、网络安全管理和大客户业务管理等功能的建设。

河南移动南阳公司 CMNET 网络将采用简单开放的业务策略，具备支持多种业务的能力。目前主要开放 3 类重要业务，即有质量保证的企业互连和大客户专网、移动互联网业务以及集团客户互联网上网业务。

3.2.2.3 网络维护体系介绍

河南移动南阳公司作为南阳网络和用户规模最大的移动运营商，不仅网络规模是全市最大的，在网络质量上也处于全市领先水平。一流的网络离不开一流的维护，河南移动南阳公司借助高效的网络维护体系，以集中化、标准化、精细化的网络运维，达到了全市领先的网络质量和运维效率。

流程

河南移动南阳公司网络运维体系是以客户需要为导向，系统化、标准化的运维流程体系，其流程是结合 eTOM 和 ITIL 模型而设计的。河南移动南阳公司卓越网络运维体系充分借助 IT 手段固化了核心流程，明确了流程中岗位、人员与职责，大大提升了运维体系的效率。

网络管理平台

河南移动南阳公司建立了完善的全市统一集中网络管理平台，将全市无线网、交换网、数据网、传输网等基础网和业务网均纳入了管理范围，实现了全市网络运行全过程实时集中监控、性能统一分析、数据统一制作、资源统一调度、网优方案集中制定等功能，使网络管理机构相对集中，减少管理层次，实现网络快速生产指挥调度管理。

维护机制

河南移动南阳公司网络维护采取“两级集中管理、三级维护”的原则。两级

公共资源交易平台投标专用

集中管理指河南移动南阳公司和分公司，在市公司层面，市网络部负责网络维护的管理职能，市网络管理中心负责全市网络的集中管理、集中操作、集中监控等生产职责；分公司负责本地网络的维护。三级维护指河南移动南阳公司市、县、乡网络维护机构设置和维护范围的划分。

组织结构

河南移动南阳公司卓越网络运维体系具有简洁高效的运维管理模式和组织结构，分为两级集中管理、三级维护作业的生产组织模式，整个运维体系以市级维护单位为中心的、以市级维护单位为主体、以县/区级维护单位为分支，有机地整合了全市的网络维护资源，形成了覆盖全市的跨地域集中化运维管理方式。

3.2.2.4 **网络维护单位分布**

地区	所属县/区维护单位
南阳	邓州分公司
	南召分公司
	方城分公司
	西峡分公司
	镇平分公司
	内乡分公司
	淅川分公司
	社旗分公司
	市区分公司
	油田分公司
	郊区分公司
	唐河分公司
	新野分公司
	桐柏分公司

3.2.2.5 **传输专线开通服务**

专线开通时限：政府各入网单位填写业务受理单之日起，至开通专线接入服务（不包括用户设备）实际占用的时间；最长为 30 日。

专线开通标志：两端线路均按要求到达用户指定位置，采购人两端入网单位

公共资源交易平台投标专用
AE2C19CEC77...A62A8BC88EA14DB9

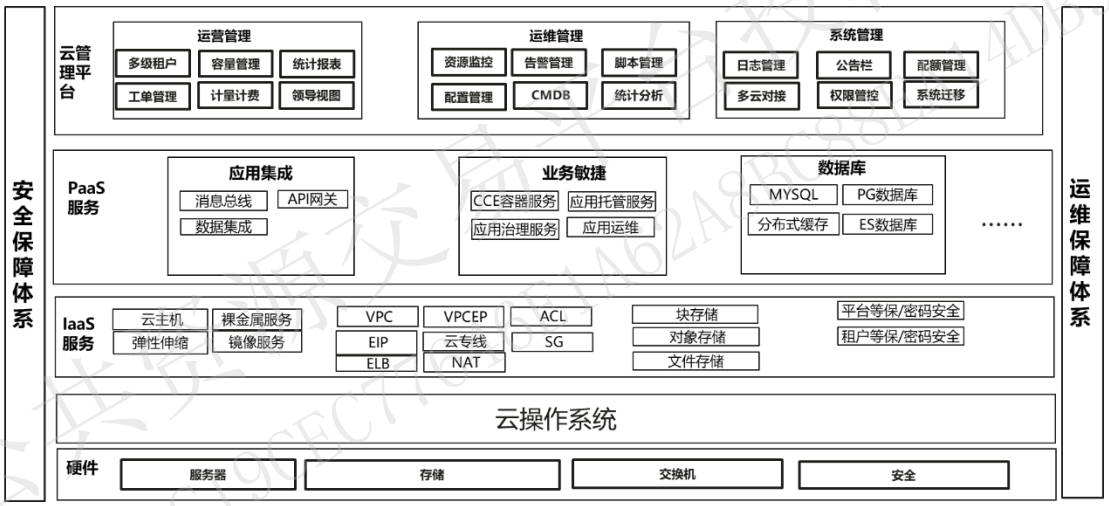
签字认可后，即视为开通。如遇特殊情况，双方可进行具体协商。

提供的服务具体标准满足工信部颁布的《电信服务规范》，保证使用通信业务安全畅通。网络可用率≥99.9%；主干环路切换时间＜50ms；端到端电路（采购人中心节点到各分支节点）的传输比特差错率（误码率）≤1.0×10E-7；全网中断次数≤20 次/年；单点中断次数≤5 次/年。故障响应时间小于 10 分钟，故障响应率达到 100%，业务恢复时限小于 4 小时（由于光缆中断、甲方原因、不可抗力、正常割接导致的专线中断除外）。

3.2.3 云底座建设方案

3.2.3.1 整体建设方案

本项目采用分层云架构设计，为云平台提供基础云平台、基础 IaaS 服务、PaaS 服务，云管理服务能能力，如下图所示：



系统服务架构

通过华为云 Stack 云操作系统，实现对底层服务器、存储、网络设备、安全设备的统一纳管、配置以及虚拟化处理。形成云平台底座资源池。

IaaS 服务主要提供计算、存储、网络、安全四大服务能力。为云平台业务以及高阶 PaaS 服务提供底层计算和服务能力。

PaaS 层主要提供应用集成服务（如消息总线、API 网关、数据集成服务），应用敏捷管理服务（如应用托管、微服务治理、应用运维服务、容器服务），数据库服务（如 MYSQL，PG，ES，分布式缓存等）

云管理平台主要提供运营管理和运维管理能力。

本项目架构按照《中华人民共和国网络安全法》、《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）等法律规范建设平台安全体系，从物理安全、网络安全、主机安全、数据安全和应用安全等多个层面，确保云平台符合安全合规要求，提供具体的云平台网络安全服务方案等，全面保障云平台的安全。

本项目架构按照《中华人民共和国密码法》、《信息安全技术信息系统密码应用基本要求》（GM/T39786-2021）等法律规范建设平台密码安全体系，提供云平台商用密码应用安全服务方案，规范密码的使用和管理，提供坚实可靠的网络安全密码保障。

3.2.3.1.1 建设原则及依据

在建设过程中，明确政务云平台不仅仅是简单地把各种应用系统集中在机房里，而是通过提供统一的云计算环境，弹性地为各政务部门提供各种计算环境，为各种应用提供了一个安全、可靠、弹性、高可靠的框架和服务，各个应用系统集中地共享各种机房基础设施资源，有效降低建设和运行成本，使得电子政务的服务能力有效提升，从而推进科技创新在政务领域的示范应用。

平台的方案规划、设计思路如下：

（一）高性能

本方案提供的弹性计算服务，能够提供基本水平的 vCPU 性能，平衡计算、内存和网络资源，同时可根据工作负载的需要实现性能的突增，具有短期发挥更高性能的能力，能满足核心应用场景对高性能、稳定性、高安全性的需求。提供高带宽支持，能随时升级网络以满足将来的业务需要，包括提供多种接入端口等。提供高性能企业级数据库，采用计算存储分离架构，可实现超百万级 QPS 吞吐，支持跨 AZ 部署，数据 0 丢失。提供高性能的云硬盘存储，对象存储，文件存储。提供高性能的组网架构，满足数据中心对数据吞吐和交换能力的要求，具备应对峰值流量的能力。

（二）高可靠

本方案云基础设施的建设采用可靠的架构和体系。云计算平台采用先进的设计思想和方法，符合技术发展趋势。本方案云计算平台既可以适应地理环境、应用场景、运维能力以及投资规模等客观因素，又可以灵活地配置云服务种类和硬

公共资源交易平台技术专用

件、网络，具有较高的性价比，满足业务管理可靠的需求。同时，云计算平台应该经受过高并发、高可靠的实践验证，确保采用的技术体系是经过更大的适用范围验证过的。

（三）高安全

本方案严格按照等保 2.0 等国家及行业安全标准规范设计建设，遵照各级保密法律法规，并采用相关的软件技术提供较强的管理机制、控制手段和事故监控与安全保密等切实有效的措施，确保系统安全稳定运行。

（四）易管理

本方案的易管理性主要体现在实用的功能设计和 UI 设计上，合理的交互性设计是提供易用性的主要手段，让最终用户操作简单、使用方便、可集中管理和易于维护也是云平台易用性需要衡量的标准。 租户是计算机资源、云平台界面信息的使用者，根据各租户的习性，技能、知识和经验设计出的交互系统更适合于用户的使用。云平台界面是人机之间的信息界面，交互是一个结合计算机科学、美学、心理学、人机工程学等工业和商业领域的行为，其目标是促进设计、执行和优化信息与通信系统以满足政府用户的需要。

（五）标准化

本方案的建设采用云计算资源池建设模式，充分考虑既有系统搬迁和新系统建设需求，所有资源整合后在逻辑上以单一整体的形式呈现，这些资源根据需要进行动态扩展和配置，支撑企业按需使用。在存储资源建设方面，提供大规模横向扩展能力，提供的基础设施，提供标准化的扩展能力，在评估和测试过的兼容性基础上，能够互连不同制造厂商的设备，实现计算机软、硬件资源的数据交换。

（六）统一性

本方案遵循国家电子政务的要求，以系统工程的方法对系统进行统一规划、统一设计，遵循统一的规范，采用统一的技术，以方便系统建成后的运行和维护，保证系统可持续、高效、安全运行。

（七）自主可控

随着国家等保 2.0、安可等政策的推行，平台及平台之上的应用和数据安全成为云平台建设重点保障对象。云平台的建设，云服务商充分贯彻国家相关安全政策法规，已通过国产 ARM 芯片、国产欧拉操作系统、国产基础软件等技术全面

实现国产化替代，满足信创和安可等要求。

（八）绿色节能

本方案提供先进的基础设备，满足绿色节能减排的标准要求，利用先进的云计算平台技术，例如虚拟机热迁移技术，不但能保证虚拟机的可用性，规避业务中断的风险，还能降低客户的业务运行成本，达到了节能减排的作用。

3.2.3.1.2 物理组网架构建设方案

基于政务云数据中心的高安全性、高扩展能力和可管理性的业务需求，云数据中心网络架构的总体规划遵循结构化、模块化和层次化的设计理念，实现网络层次更加清楚、功能更加明确，数据资产更加安全和管理更加方便。

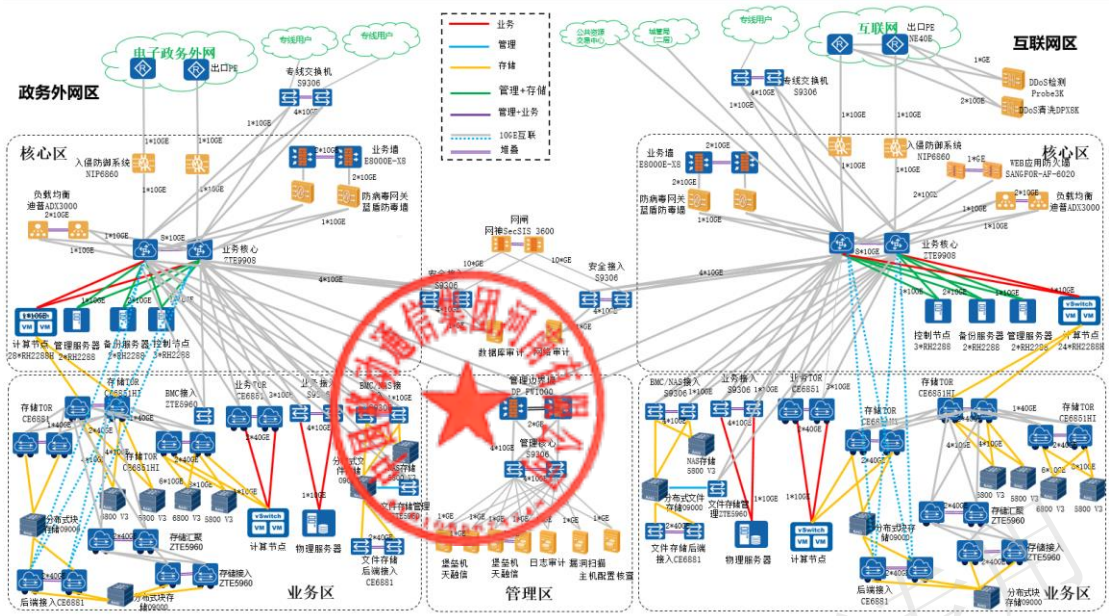
第一，结构化：结构化设计便于上层协议的部署和网络的管理，提高网络的收敛速度，实现高可靠。云中心网络结构化设计体现在适当的冗余性和网络的对称性两个方面，一般采用双节点双归属的架构实现网络结构的冗余和对称，可以使得网络设备的配置简化、拓扑直观，也有助于协议设计分析。

第二，模块化：模块化的设计方法，将数据中心划分为不同的功能区域，核心区用于承接各区域之间的数据交换，是整个云中心的核心枢纽，各接入区用于不同类应用的分类接入。服务器根据应用功能、用户访问特性、安全等级等要求部署多个区域，使整个云中心的架构具备伸缩性和灵活性，同时也便于安全域的划分和安全防护的设计实施。

第三，层次化：随着接入交换机性能和密度的提升，以及服务器虚拟化的广泛使用，网络结构设计可采取两层扁平结构，分为核心层和接入层。通过分层部署可以使网络具有很好的扩展性，无需干扰其它区域就能根据需要增加接入容量，提升网络的可用性，隔离故障域，降低故障对网络的影响范围，简化网络的管理。

第四，可扩展：本次数据中心的网络方案，支持未来容量上的扩容，同时支持网络结构上的扩展，支持后续两地三中心（本地双活，异地容灾）的演进。

本项目的云平台网络架构，按照不同的功能进行区域划分，如下图所示：



云平台网络部署架构

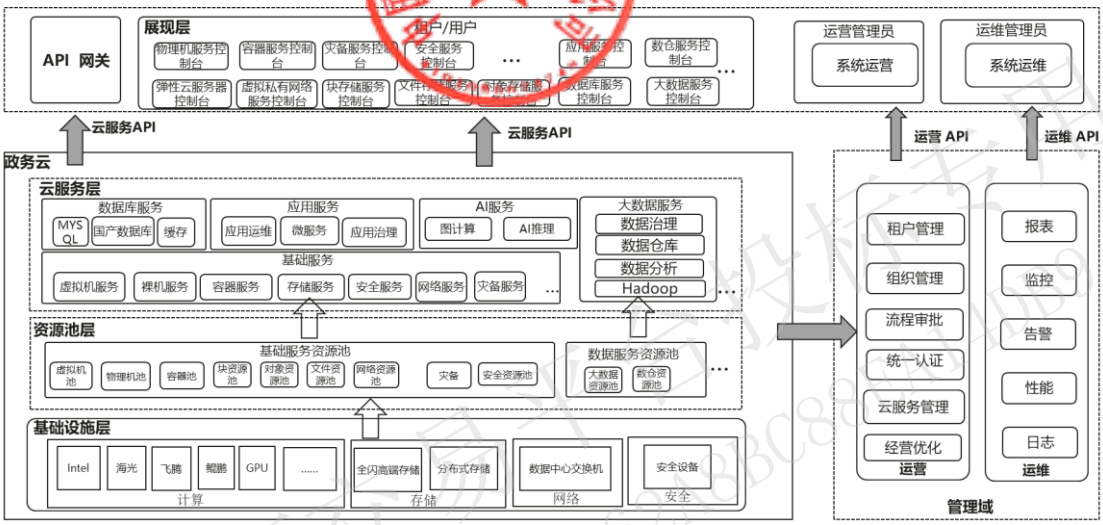
本项目整体采用 10G 组网，上行到核心交换机采用 40G 接口。公网出口采用 10GE 吞吐量设计，专线出口采用 10G 吞吐量设计，可以按需扩容；运维出口采用 10GE 吞吐量设计。本项目采用分区设计原则，分为政务外网区和互联网区，政务外网区和核心区共管理区，管理区负责政务外网区和核心区的统一管理，政务外网区和核心区通过网闸进行数据交换。

1. 互联网出口区，互联网出口区部署AntiDDOS，出口防火墙、出口IPS设备，用于互联网出口的安全防护。
2. 核心区部署核心防火墙，密码机、SSL VPN、平台漏洞扫描设备用于防护云平台的边界安全和计算安全。
3. 运维管理区，运维管理区部署运维接入防火墙以及BMC交换机等，实现运维安全防问。
4. 存储区，影响存储区采用双活部署在不同的两个机房， 通过L3GW实现与云内业务的互通。
5. OBS区，OBS区主要用于云平台的备份以及一些OBS文件的存储。
6. SFS区，文件存储区主要用于NFS等文件协议的访问，提供文件存储服务。
7. 虚拟化业务区，虚拟化业务区部署计算节点、网络节点、EP节点、备份节点等。

8. 裸金属业务区部署裸金属服务，部署2台裸金属网关用于裸金属的SDN网络访问能力。
9. 云平台管理区，部署云平台管理组件、平台安全组件、服务Console,公共服务组件等。

3.2.3.1.3 平台逻辑架构建设方案

本项目云平台总体架构如下图所示，主要由基础设施层、资源池层、云服务层、展现层和管理域组成。



系统功能架构

基础设施层指的是云平台实际运行的物理设施，包括飞腾、海光、X86、ARM或者包含GPU的计算服务器，提供块存储的SAN或者分布式存储设备，提供对象或者文件的存储设备，然后这些设备的单台设备（包含计算服务器和存储服务器），通过网络交换机、路由器、防火墙组网互联起来，从而形成大规模集群；这些大规模集群在云平台的管理下，为上层业务提供具有云平台能力的资源服务使用方式。

资源池层是个偏逻辑的概念，将基础设施层提供的硬件设备按照逻辑功能的不同划分为不同功能的资源池。按照提供服务能力的不同可以分为基础服务资源池和数据服务资源池；基础服务资源池可以接入计算（虚拟机池、裸金属池、容器池）、存储（块存储资源池、对象存储资源池、文件存储资源池）、网络资源池、安全资源池、灾备资源池。数据服务资源池可以接入大数据资源池和数据仓库资源池。各种资源池可以根据项目需要进行按需构建，每种类型的资源池可以配置

一个或多个，也可以对不需要的资源池进行裁剪。

云服务层作为云服务的后端实现实体，主要完成服务的封装和对资源的自动化分配、使用。通过对资源池层相关资源的封装，实现云资源服务的发现、路由、编排、计量、接入等功能，实现从资源到服务的转换。

展现层是云管理平台的对外呈现，分为用户门户及管理员门户。用户门户面向最终租户/用户，管理员门户面向系统运营/运维管理员等。租户/用户可通过服务控制台自助实现对服务的申请、使用、监控、删除等生命周期管理的操作。运营/运维管理员可以通过管理员门户完成对系统的管理。

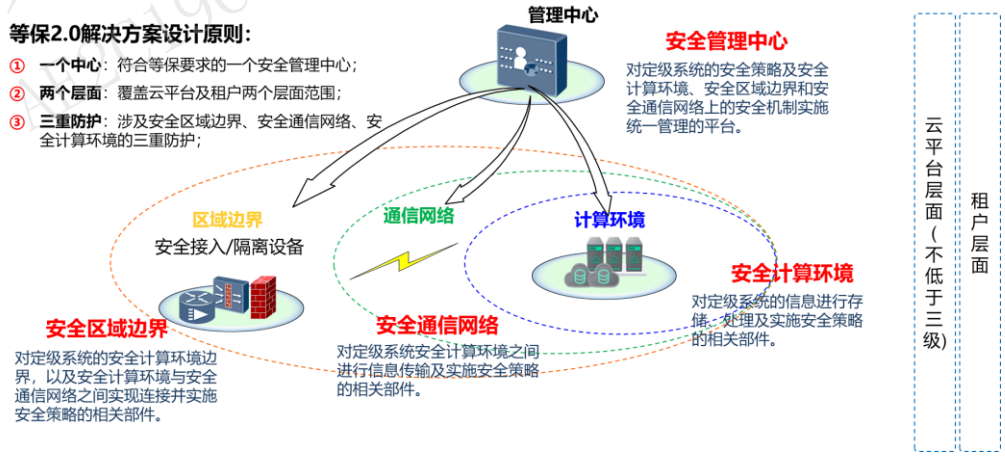
统一 API 网关，系统通过 API 网关开放系统的云服务和管理 API ，并提供应用 APIG，业务系统可以通过 API 网关，实现云服务能力的二次加工和使用。

运营管理，提供运营管理功能，运营管理可以提供云服务申请和自助服务能力，包括租户管理、组织管理、流程审批、统一认证、云服务管理、经营优化等运营管理功能。

运维管理，提供运维管理功能，支持对多数据中心的统一运维管理，包括告警、性能、监控、日志以及报表等功能。

3.2.3.1.4 安全架构建设方案

华为云 Stack 提供完整的等级保护解决方案，通过“一个中心”+“三重防护”的安全服务和内置安全能力，满足等级保护要求，并按照套餐模式向客户提供一站式等级保护解决方案。



等保解决方案原则

1、**一个中心**：建立集中的安全管理，通过统一认证、统一鉴权、统一审计、数据脱敏、数据泄露检测等管理等手段，实现集中的安全认证、安全审计、安全

公开资源交易平台技术专用

监控。

2、**三重防护：**

- 基础设施安全防护

基础设施环境是对云平台的自身的安全防护措施，包括网络、边界区域、云平台自身、主机、应用层等的安全防护，主要包括防火墙、DDoS、IPS、APT、AV等安全防护措施。

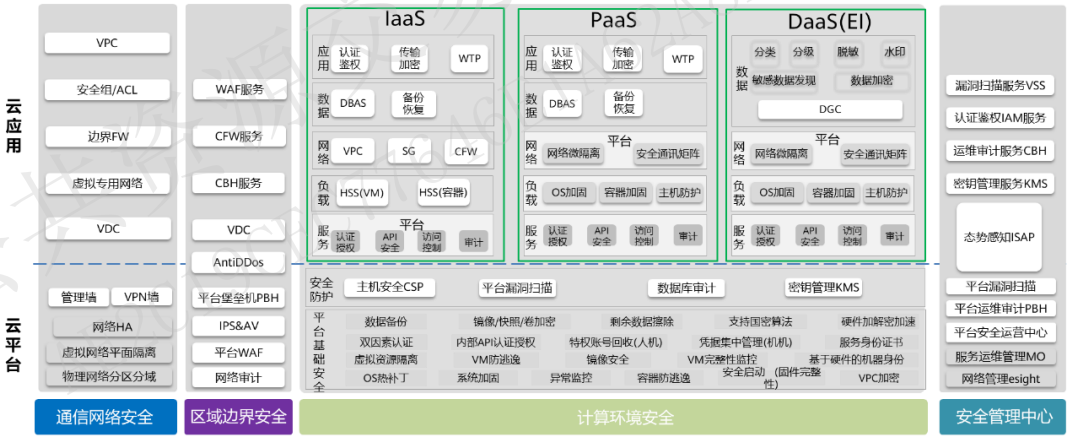
- EI平台安全防护

主要是针对 EI 平台自身的安全防护，如漏洞管理、系统加固、恶意代码防范、数据备份等，通过平台侧对系统、对主机、对数据进行实时的安全管理和监控。

- 数据安全方案

数据的生命周期包括数据采集、数据传输、数据存储、数据使用、数据共享、数据销毁六个阶段

3、**六个阶段**：提供数据全生命周期的安全防护，覆盖了数据全生命周期的六个阶段，即数据采集、数据传输、数据存储、数据共享、数据使用、数据销毁。



云平台网络部署架构

1、等保整体解决方案设计原则为“一个中心+三重防护“，安全能力覆盖租户和平台；面向业务提供可满足等保认证的安全套餐；

2、平台安全能力由平台基础安全和平台安全服务注册，基础安全为内置能力，安全防护通过安全服务产品提供支持；

3、租户安全方案由服务内置安全和安全服务组成，租户自研应用需要基于安全服务的能力构建租户应用安全；

4、其中 AntiDDos、态势感知、日志审计服务可同时支撑平台和租户，无需分别单独部署；

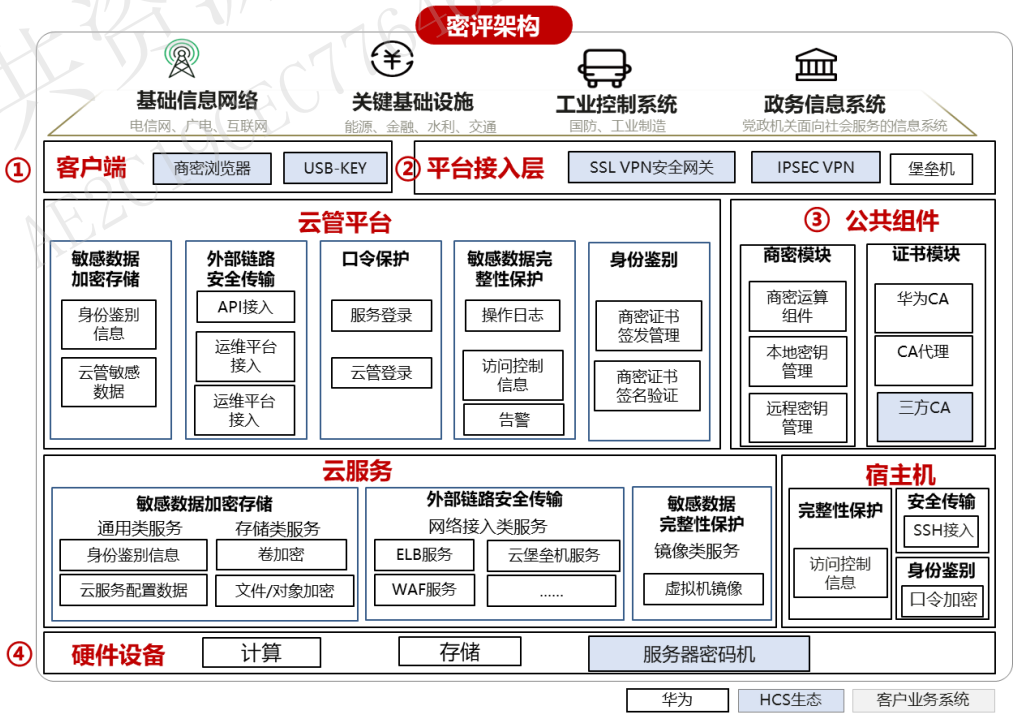
5、在通信网络安全中，通过网络分区隔离、虚拟网络平面隔离、管理墙、VPC、云防火墙、网络高可靠等技术能力，满足等保安全通信网络要求；

6、在区域边界安全中，通过 AntiDDos、IPS&AV、WAF、云防火墙等技术能力，满足安全区域边界中边界防护、访问控制、入侵检测、安全审计等技术要求；

7、在技术环境安全中，通过平台基础安全、平台安全防护、主机容器安全服务、网络隔离服务、认证鉴权服务、应用防护服务，满足等保认证中身份鉴别、访问控制、入侵防护、数据保护等技术要求；

8、在安全管理中心中，通过日志审计、态势感知、数据安全管理、运维审计、密钥管理、漏洞扫描等，满足等保认证中系统管理、审计管理、安全管理、集中管理等技术要求；

为满足 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，密评改造涉及对华为云增加密码运算公共组件、设备用于支撑以下方面改造，技术难度大，涉及面广 ：1.本地凭据、敏感数据存储加密，2.外部链路 https 安全传输，3.登录口令 Hash 保护，4.访问控制信息、日志等完整性保护，5.服务接入身份鉴别，6.密钥、证书管理



云平台密评安全架构架构

华为云平台密评方案优势：

- 一站式服务：提供咨询+产品+测评能力，全流程质量监督管控，专家深度参与
- 云原生密评改造能力：密码安全服务按需选配，标准化、易交付、易维护
- 业务使能：KMS、WAF、云堡垒机、弹性负载均衡、VPN等服务面全面支持国密算法

3.2.3.1.5 可扩展性建设方案

本项目为云平台提供的云平台具备强大的扩展能力，打造统一的云管理平台，业务可以按需分省分区进行 REGION（区域）的扩展，同时在 REGION 内，也可以按照 AZ 的方式进行扩展。

本项目提供的云平台可以满足单 REGION 内扩展 2000 台服务器能力，得益于华为强大的 SDN 调度技术，可以实现超大规模性网络的高效率控制，满足超大型数据中心云平台扩容需求。

本项目提供的存储，采用分布式存储技术，单集群可以支持上千台分布式存储节点扩展，实现 100PB 级扩容能力，可以满足云平台业务的发展诉求。

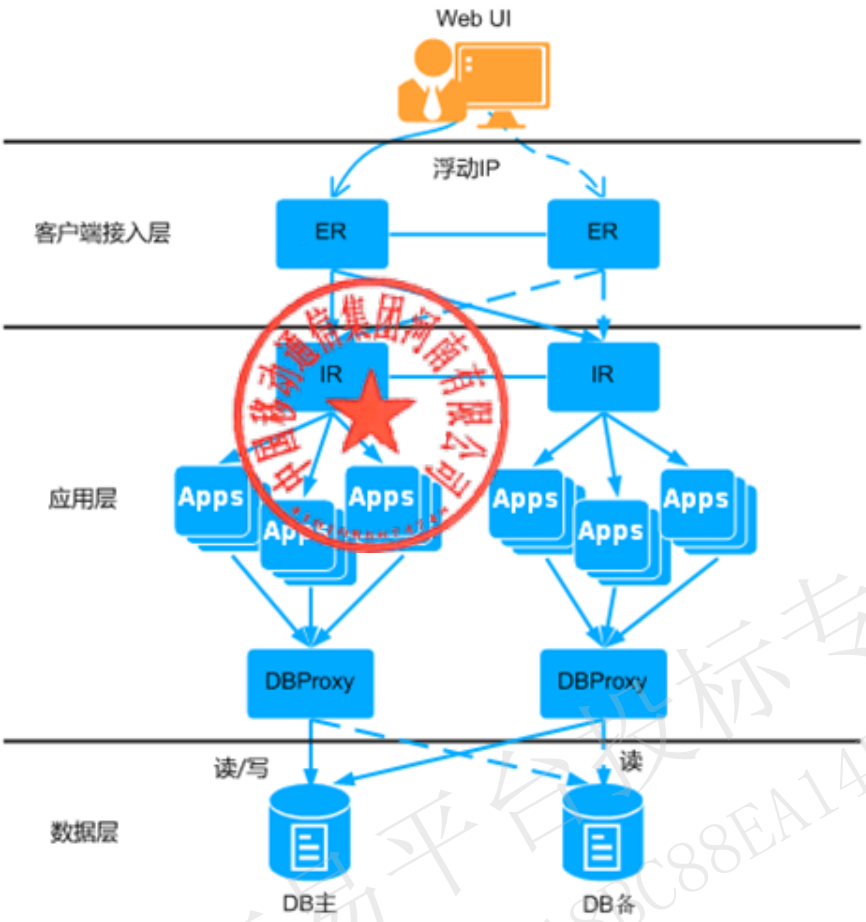
对于单个虚拟机而言，通过华为强大的虚拟化技术，可以实现单个虚拟机扩展 16 块网卡，挂载 60 块存储卷的扩展能力，在业界处于领先地位。

3.2.3.1.6 可靠性建设方案

3.2.3.1.6.1 管理面高可靠

云平台管理面采用多节点冗余部署，管理面 VM 采用反亲和方式部署在管理节点上，保障云平台管理面高可靠。

公共资源交易平台技术专用



云管理平台高可靠

ManageOne软件系统各层的可靠性措施如下所述：

- 客户端接入层

浮动IP地址保证故障切换前后对用户IP地址不变，减少用户对故障切换的感知。

- 应用层

  - 应用进程无状态集群是微损切换的基础。

  - 请求响应总线对故障的应用节点自动隔离。

  - DBProxy路由数据请求到主用数据库，降低应用进程对数据服务故障切换的感知，简化应用开发。

- 数据层

  - 健壮的数据服务支撑应用的无状态化，应用将状态数据外置到数据

公共资源交易平台投标专用

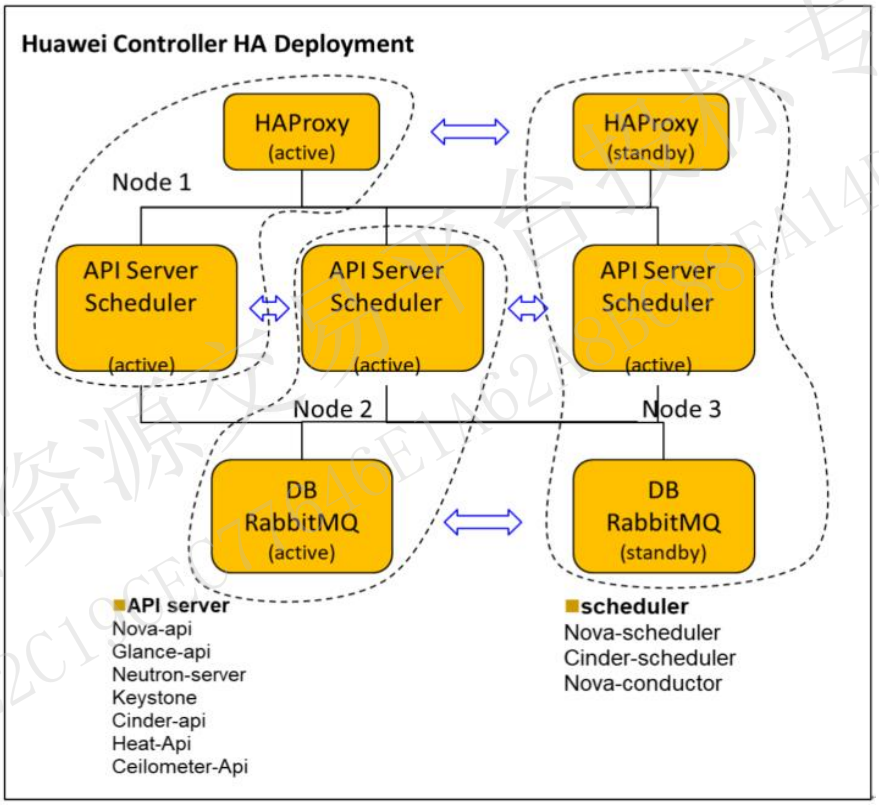
服务。

– 数据服务热冗余双活，主备之间日志同步复制，支持故障自动快速微损切换。

3.2.3.1.6.2 资源层高可靠

基于华为 OpenStack+KVM 构建，保障对外提供服务功能的可靠性，主要包含以下几个部分：

- Rest API服务可靠性，为用户提供不中断的API服务。
- 数据库服务可靠性，保证用户配置数据不丢失，服务不中断。
- 通讯服务可靠性，保证组件间交互正常不中断。



资源层高可靠

- HAProxy负责Rest API服务的负载分发，支持部署成active-standby模式；
- API Server和Scheduler提供无状态服务，通过负载均衡方式提供服务，支持部署成active-active模式；
- DB为Gauss数据库，采用热主备方式，支持部署成active-standby模式；

- RabbitMQ采用热主备方式，支持部署成active-standby模式；
- 网络节点支持部署成active-active模式；
- 计算节点支持部署成active-active模式；

3.2.3.1.6.3 计算可靠性

虚拟机热迁移

为保证虚拟机的可用性，规避业务中断的风险，系统提供虚拟机热迁移能力，即虚拟机在不中断业务的情况下实现迁移。虚拟机迁移时，管理系统会在迁移的目的端创建该虚拟机的完整镜像，在源端和目的端进行同步。同步的内容包括内存，寄存器状态，堆栈状态，虚拟 CPU 状态，存储以及所有虚拟硬件的动态信息。在迁移过程中，为保证内存的同步，虚拟机管理器（Hypervisor）提供了内存数据的快速复制技术，从而保证了在不中断业务的情况下将虚拟机迁移到目标主机（图示如下）。同时，通过共享存储保证了虚拟机迁移前后持久化数据不变

虚拟机 HA

当计算节点宕机或者虚拟机状态为 error，系统可以将具有 HA 属性的虚拟机故障迁移到其他健康的计算节点，保证虚拟机能够快速恢复。

虚拟机故障检测

当虚拟机本身发生故障虚拟机出现异常挂死的情况时，系统能够检测并本地重启尝试恢复。

3.2.3.1.6.4 网络可靠性

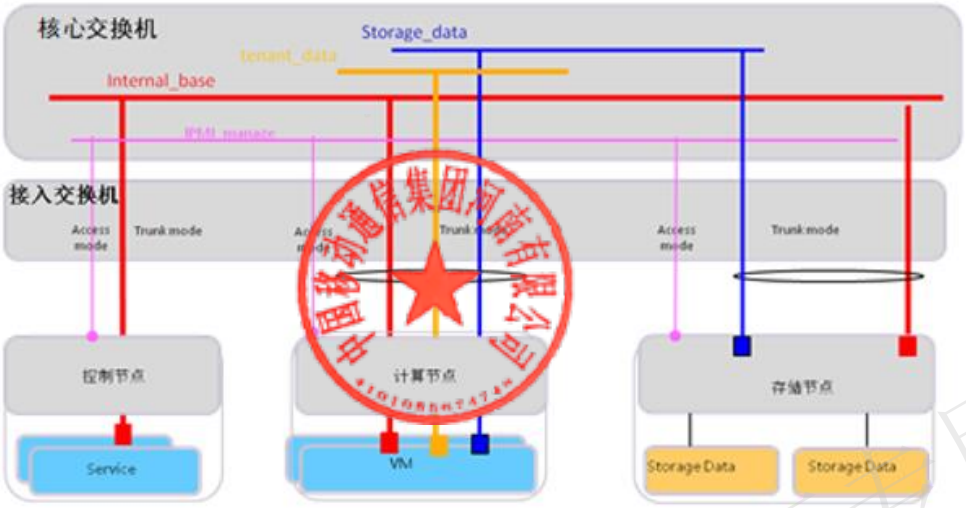
网络平面通信

系统通信平面逻辑上可以分为四类平面：管理平面、存储平面、业务平面和 IPMI 平面。其中：

- 管理平面网络：用于承载业务节点之间的API/RPC消息流量。
- 业务平面网络：用于承载虚拟机业务数据。
- 存储平面网络：用于承载存储平面内的存储数据互连。
- IPMI平面：用于承载服务器硬件管理消息。

为了保证各种网络平面数据的可靠和安全，云平台采用多网络平面的架构方案，不同平面间采用 VLAN 进行隔离，单个平面的故障不影响其他平面继续工作。例如当管理平面暂时故障时，业务平面还能够用于继续访问虚拟机。此外，系统

还支持基于 VLAN 的优先级设定，使得内部的管理/控制报文具备最高的权限，出现拥塞时，管理员和用户均可以管控系统。



网络平面划分

在服务器内部，可通过对多个网卡的合理绑定和分类，允许将管理、业务和存储平面部署在不同物理网卡上，并将其连接到不同的接入层交换设备接口上，从而实现物理层面的网络隔离。

交换机高可靠

本项目的数据中心交换机采用 M-LAG（Multichassis Link Aggregation Group）即跨设备链路聚合组，M-LAG 是一种实现跨设备链路聚合的机制，将一台设备与另外两台设备进行跨设备链路聚合，从而把链路可靠性从单板级提高到了设备级，组成双活系统。

M-LAG 作为一种跨设备链路聚合的技术，除了具备增加带宽、提高链路可靠性、负载分担的优势外，还具备以下优势：

- 更高的可靠性:把链路可靠性从单板级提高到了设备级。
- 简化组网及配置:可以将M-LAG理解为一种横向虚拟化技术，将双归接入的两台设备在逻辑上虚拟成一台设备。M-LAG提供了一个没有环路的二层拓扑同时实现冗余备份，不再需要繁琐的生成树协议配置，极大的简化了组网及配置。
- 独立升级:两台设备可以分别进行升级，保证有一台设备正常工作即可，对正在运行的业务几乎没有影响

公共资源交易平台投标专用

3.2.3.1.6.5 存储可靠性

华为分布式存储系统通过集群冗余或主备冗余模式确保软硬件部件出现故障后系统仍能够提供服务，同时通过管控与业务面分离、存储池隔离等实现故障域隔离。

华为分布式存储系统提供了数据跨节点/机柜的保护能力，在多个硬盘、节点、机柜故障时也能继续提供服务。

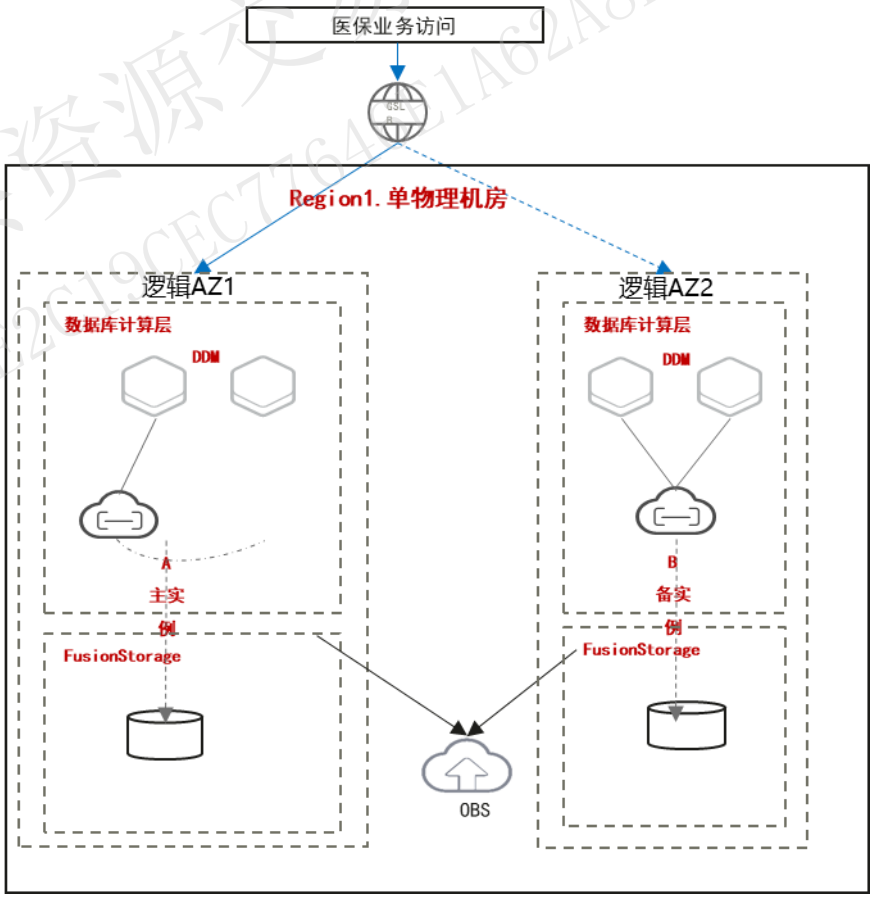
华为分布式存储系统提供支持灵活的数据布局策略，包括节点级安全布局和机柜级安全布局。

华为分布式存储池采用分区打散机制，即副本/EC 分条数据会按照策略打散到不同的服务器的不同硬盘。当华为分布式存储检测到硬盘或者节点硬件发生故障时（长时间离线），自动在后台启动数据修复。

3.2.3.1.6.6 数据库可靠性

3.2.3.1.6.6.1 关系型云数据库MySQL

MYSQL 采用主备方案部署，主备资源部署在不同的计算节点上以及不同的后端存储池上，如下图所示：



公共资源交易平台投标专用

MySql主备方案

MYSQL 主备部署支持设置可靠性优先和可用性优先。

可靠性优先：数据完整性要求高，主库数据没有完全同步到备库时，不允许主备倒换

可用性优先：系统可用性要求高，主库数据没有完全同步到备库，在一定条件下，也可以主备倒换

MySQL 可靠性优先/可用性优先手动倒换：没有主备延迟情况下，手动倒换的业务中断时间在 1 到 3 秒内。故障切换的业务中断时间耗时 1 分钟以内。

MySQL 可靠性优先自动倒换：自动倒换的前提是主库故障，HA 判断主库故障 -> 等待备库和主库数据一致 -> 将备库升主库 -> 备库绑定数据 VIP 和管理 VIP

主备同步有延迟，不能备库升主库，会一直维持双备，期间主库恢复，会继续是主库；同时会有告警，需要人工介入

MySQL 可用性优先自动倒换：自动倒换的前提是主库故障，HA 判断主库故障 -> 确保主库和备库数据差小于 5 分钟 -> 将备库升主库 -> 备库绑定数据 VIP 和管理 VIP(5 分钟计算方式：show slave status 里的 seconds_behind_master)，如果主备数据差大于 5 分钟，就等备库继续重放 relaylog。如果超过 5 分钟还未完成，就是双备的选主的过程。只要发现小于 5 分钟就会开始倒换，丢失 5 分钟或者小于 5 分钟的数据是必然的，如果主备有时间差，会把没有重放完成的 binlog 保存到 OBS 上，作为备份保存起来。

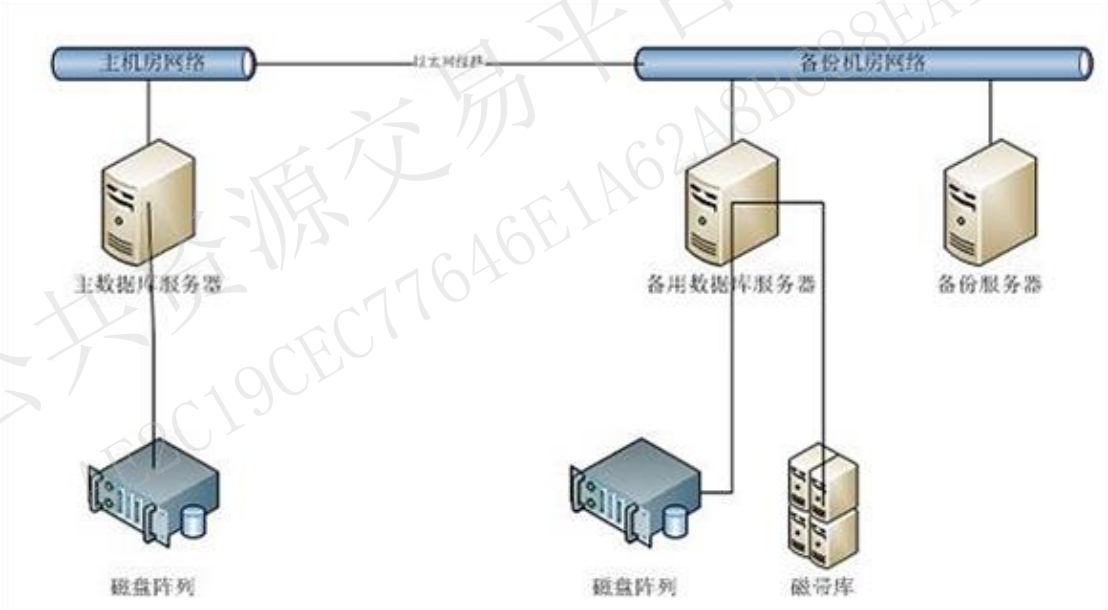
3.2.3.1.6.6.2 关系型云数据库Oracle

Oracle 数据库是一款高度可靠的企业级数据库系统。其可靠性主要体现在以下几个方面：

- **高可靠性：**Oracle数据库具有高度可用的特性，它采用了诸如RAC(Real Application Cluster)等高可靠性技术，可以在处理海量数据时保持稳定性。RAC允许在多台服务器上运行多个数据库实例，以提高系统的可用性和故障恢复能力。
- **数据保护：**Oracle提供了多种数据保护功能，如数据备份和恢复、闪回等。这些功能可以帮助企业在发生故障或错误时快速恢复数据，并确保

数据的完整性和一致性。

- **稳定性：**Oracle数据库在稳定性方面表现出色。它采用了许多优化技术来提高性能和稳定性，例如自动存储管理(A)和Database Replay等。这些技术可以帮助企业确保系统的高可靠性和稳定性。
- **安全性：**Oracle数据库具有严格的安全性控制机制，包括用户认证、访问控制和数据加密等。这些功能可以帮助企业保护数据的安全性和完整性，防止未经授权的访问和恶意攻击。
- **可扩展性：**Oracle数据库具有良好的可扩展性，可以随着企业的业务增长而平滑地扩展性能和容量。它支持各种硬件和软件平台，并可以通过添加更多的服务器和存储设备来提高系统的性能和容量。
- **异地灾备：**支持创建异地灾备库，通过数据传输实现异地数据实时同步，在突发状况下，用户可将异地灾备库切换为主库，保障业务可用性。

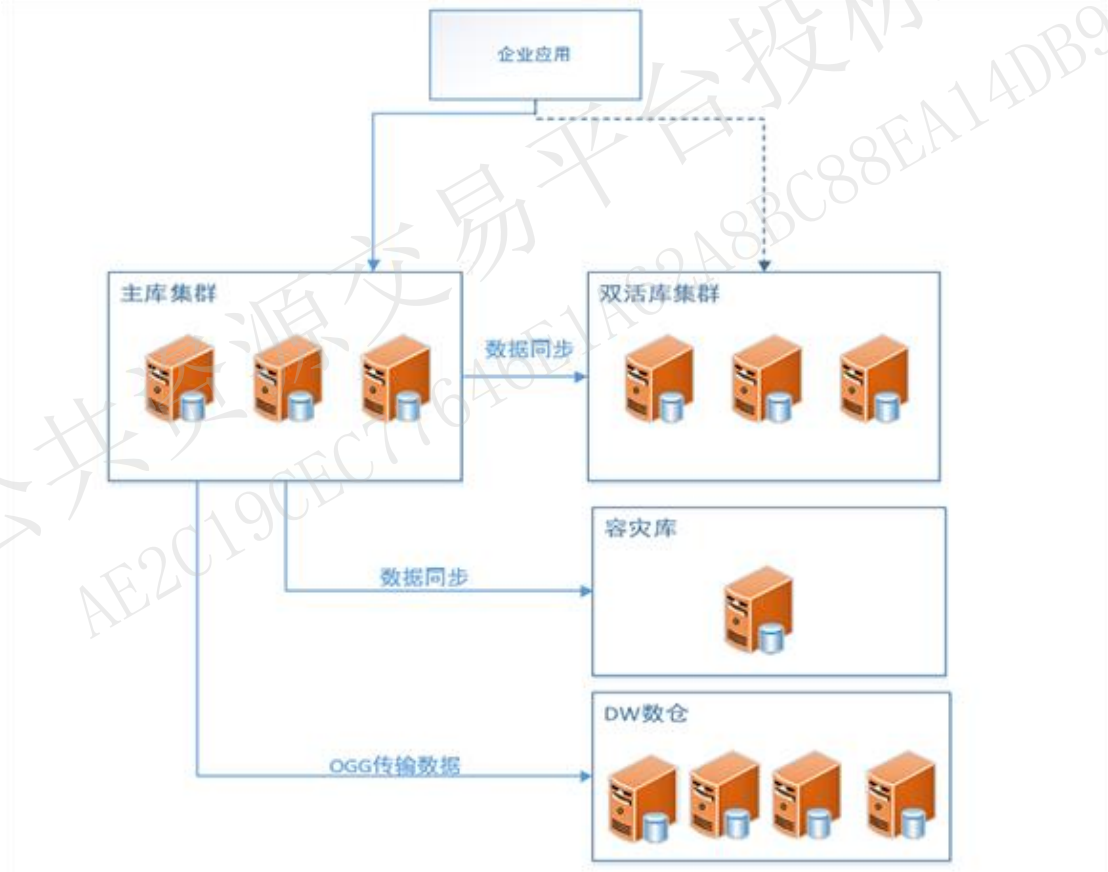


- **读写分离：**针对多读少写,有IO性能瓶颈的大型数据库，使用inmemory后性能明显提升。 应用程序在使用inmemory特性上和使用传统的Oracle数据库并无二样，不需要特殊开发或设置。

公共资源交易平台投标专用
E2C19CEC77646E1A62A3B088EA14DB9



- **同城双活：**可以在同城内的两个数据中心之间实现数据同步和备份，保证数据的一致性和完整性，同时提供高可靠性和容灾能力。可以将应用负载均衡到两个数据中心上，以提高系统的可用性和性能。可以使用虚拟机HA技术来实现业务的连续性，当一个数据中心发生故障时，可以自动切换到另一个数据中心。



3.2.3.1.6.6.3 **关系型云数据库SQL Server**

SQL Server 提供了多种高可靠性解决方案，其中包括：

公共资源交易平台投标专用
AE2C19CEC7164E1A82A8BC88EA14DB9

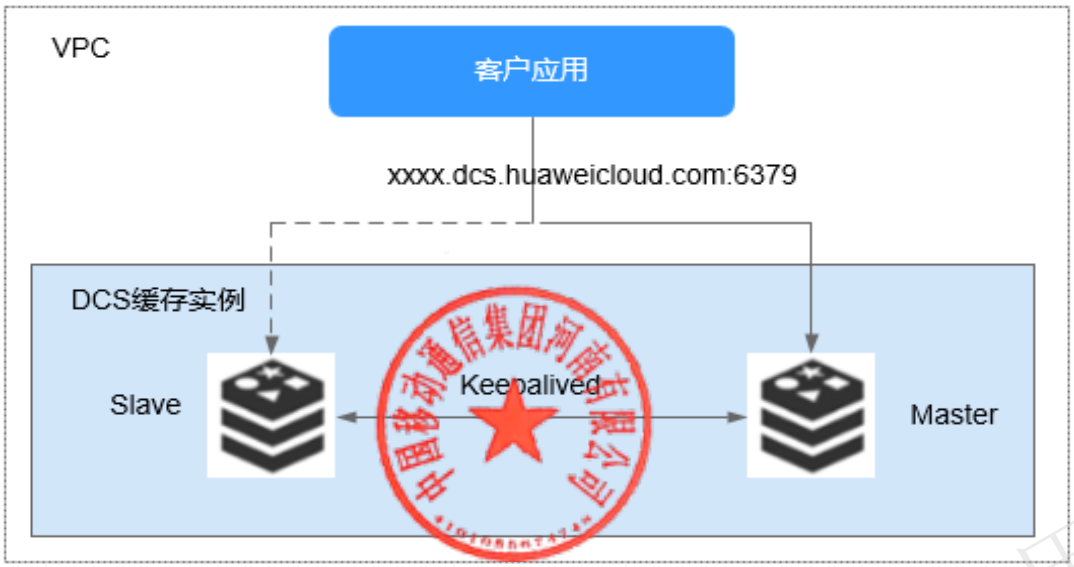
- AlwaysOn 可用性组：通过将多个数据库服务器组成一个可用性组，实现数据库的自动故障转移和故障恢复。可用性组中的主服务器处理读写操作，而辅助服务器则充当备份服务器，当主服务器发生故障时，辅助服务器会自动接管服务。
- 数据库镜像：将数据库的完整副本保持在两个或多个服务器上，并实时同步数据的变化。当主服务器发生故障时，镜像服务器可以快速接管服务。
- AlwaysOn 可用性组和数据库镜像的结合：通过将 AlwaysOn 可用性组与数据库镜像结合使用，可以实现高可靠性和数据保护的双重保障。
- AlwaysOn 故障转移群集：通过将多个数据库服务器组成一个故障转移群集，实现数据库的自动故障转移和故障恢复。当主服务器发生故障时，群集中的其他服务器会自动接管服务。
- AlwaysOn 可用性组和故障转移群集的结合：通过将 AlwaysOn 可用性组与故障转移群集结合使用，可以实现高可靠性和灾备的双重保障。

除了以上解决方案外，还可以使用数据库备份和恢复、事务日志备份和恢复、数据库复制等技术来实现 SQL Server 的高可靠性。

3.2.3.1.6.6.4 **缓存数据库 Redis**

DCS 采用主备方式部署，主备实例包含了 Master 和 Slave 两个节点。默认开启数据持久化功能，同时保持节点间数据同步。DCS 实时探测实例可用性，当主节点故障后，备节点升级为主节点，恢复业务如下图所示：

公共资源交易平台投标专用



DCS主备部署方式

3.2.3.1.6.6.5 **关系型数据库 PostgreSQL**

PostgreSQL 是一个开源的、关系型数据库管理系统，具有高度的可扩展性、可靠性和安全性，因此被越来越多的开发者所青睐。

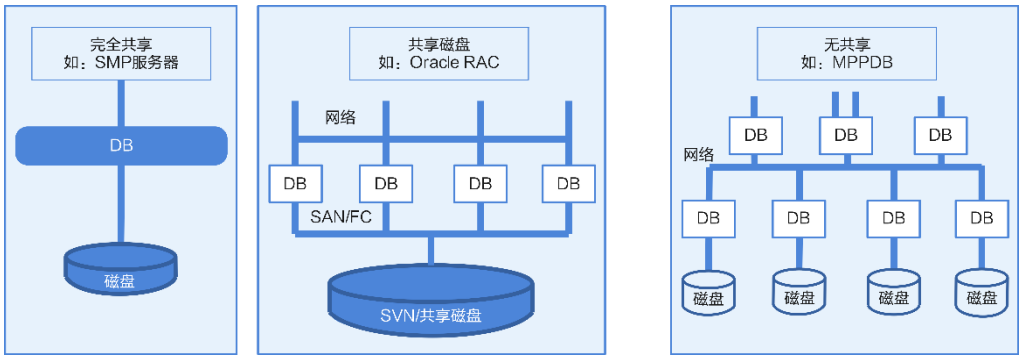
1. **ACID 四大属性**：PostgreSQL 采用完全稳定的 ACID（Atomic，Consistent，Isolated，Durable）四大属性，保证事务安全可靠。
2. **多处理器平台支持**：PostgreSQL 可以支持多处理器平台，同时有多重备份方式，实现了数据及时备份，以及完整的安全模式，严格的访问控制机制，包括身份认证验证以及审核跟踪。
3. **强大的拓展能力**：PostgreSQL 可以方便地调用本地代码，支持动态库，允许在复杂查询中轻松插入用户定义的函数，也可以使用 PL/SQL 和 PL/pgSQL 等语言编写存储过程。
4. **广泛的技术支持**：PostgreSQL 拥有广泛的技术支持，技术专家可以提供全方位的服务，从环境构建、数据库细节优化到性能测试，用户可放心的使用数据库。
5. **数据一致性和完整性**：PostgreSQL 提供了多种数据完整性检查和数据一致性保证机制。例如，它支持事务，确保数据的完整性和一致性在并发操作中得到保护。此外，PostgreSQL 还提供了强大的约束和触发器功能，可以确保数据的一致性和完整性。

公共资源交易平台投标专用

6. **备份和恢复**：PostgreSQL 支持多种备份方式，包括物理备份和逻辑备份。物理备份方式如使用 pg_dump 进行全量备份，或使用 pg_basebackup 进行实时备份。逻辑备份方式如使用 pg_dumpall 进行全量备份，或使用 pg_dump 进行部分备份。这些备份方式可以确保在发生故障时，数据能够快速恢复。
7. **高可用性**：PostgreSQL 支持多种高可用性解决方案，如主从复制、流复制、逻辑复制等。这些解决方案可以确保在主节点发生故障时，从节点能够接管，保证服务的连续性。
8. **安全性**：PostgreSQL 提供了强大的安全特性，包括访问控制、加密等。它支持 SSL 连接，可以保护数据在传输过程中的安全性。此外，PostgreSQL 还支持多种身份验证方式，如密码认证、Kerberos 认证等，确保只有授权用户才能访问数据库。
9. **监控和日志**：PostgreSQL 提供了丰富的监控和日志功能，可以帮助管理员及时发现和解决问题。例如，它支持 pg_stat_statements 功能，可以监控 SQL 语句的执行情况；支持 pg_stat_user_tables 和 pg_stat_user_functions 功能，可以监控表和函数的执行情况。此外，PostgreSQL 还支持日志记录功能，可以将操作记录到日志文件中，方便后续审计和分析。

3.2.3.1.6.6.6 分布式关系型数据库

GaussDB 是基于 Shared-Nothing 架构，它是由众多拥有独立且互不共享 CPU、内存、存储等系统资源的逻辑节点组成。在这样的系统架构中，业务数据被分散存储在多个计算节点上，数据查询任务被推送到数据所在位置就近执行，通过协调节点的协调，并行地完成大规模的数据处理工作，实现对数据处理的快速响应。



Shared-Nothing 架构具备如下优点：

- 易于扩展的架构。
  - 为 BI 和数据分析的高并发、大数据量计算提供高扩展能力。
  - 并行处理机制。
- 内部处理自动化并行。
  - 数据加载和访问方式与一般数据库相同。
  - 数据分布在所有的并行节点上。
  - 每个节点只处理其中一部分数据。
- 最优化的 I/O 处理。
  - 所有的节点同时进行并行处理。
  - 节点之间完全无共享，无 I/O 冲突。

增加节点实现性能扩展：增加节点可增加存储、查询和加载性能。

为了保证故障的可恢复，需要将数据写多份，设置主备多个副本，通过日志进行数据同步，可以实现节点故障、停止后重启等情况下，GaussDB 能够保证故障之前的数据无丢失。在一主多备模式下，所有的备机都需要重做日志，都可以升主。一主多备提供更高的容灾能力，更加适合于大批量事务处理的 OLTP 系统。

AZ 级高可用指的是同城跨 AZ 的高可用能力。客户往往会设置多个不同的可用区 AZ，将其分布在跨 AZ 的不同位置。当某个 AZ 发生断电、断网等大范围故障时，其他 AZ 仍然可以继续提供服务。GaussDB 目前提供如下几种高可用场景：同城 2AZ 高可用、同城 3AZ 高可用。

GaussDB 提供逻辑解码功能，将物理日志反解析为逻辑日志。通过 DRS 等复制中间件将逻辑日志转化为 SQL 语句，到对端数据库回放，达到双集群数据同步的功能。

GaussDB 对于分布式事务提供高可靠性，支持分布式事务强一致性，满足事务的 ACID 属性，在任何场景下不会读到分布式事务一半的数据。在同步提交场景下数据不丢失不出错，对于失败的两阶段提交事务，数据库内核提供自动化 gs_clean 服务做补偿清理，保证数据可靠及可用，即任何故障场景，无需客户手动对数据清理，数据库内部能正确处理数据提交回滚，且不会阻塞客户业务。

公共资源交易平台投标专用

集群中部署多个 CN，同时对外提供服务，增加并行处理能力。CN 的角色是对等的，即执行 DML 语句时连接到任何一个 CN 都可以得到一致的结果，而 DDL 语句需要在所有 CN 上都执行，以保持数据库对象定义一致。如果其中一个或多个 CN 发生故障，整个集群将无法执行 DDL 语句，为了避免 CN 故障影响 DDL 执行，系统支持故障 CN 自动剔除功能，在短时间内将故障的 CN 从集群中剔除，DDL 可以继续正常执行。CN 剔除后，可以通过在线节点替换命令修复 CN 并重新加入集群工作。

集群内某节点出现硬件故障造成节点不可用或者实例状态不正常，当集群没有加锁时，可通过节点替换或修复故障实例来恢复集群，修复过程中，支持用户 DML 操作，有限场景支持用户 DDL 操作。

目前企业数据规模不断增大，节点数量急剧增加，硬件损坏概率相应增加，计算节点替换修复成为日常运维工作的常态，传统的离线节点替换方式无法满足客户业务不中断需求，日常运维操作中，经常的业务中断将给客户带来重大损失。而目前业界数据库产品在节点替换的过程中，或者需要中断业务，或者只允许部分操作，均不能满足大规模数据下，常态计算节点替换的需求。

目前节点替换已支持用户业务在线 DDL：在节点替换窗口期内，已支持用户 DML 操作，有限场景支持用户 DDL 操作。

使用 gs_replace 工具可将故障节点或者实例进行替换修复。替换节点分为两种不同场景：

- 主机替换前后 IP 一致：将新主机的名称、IP 与故障主机的名称、IP 修改一致，然后做替换。适用于用户保证替换主机的名称、IP 和被替换主机的名称、IP 一致的场景，使用此方案时要求的前置条件少，能快速实现替换。

主机替换前后 IP 不一致：无需修改新主机的名称、IP，直接做替换。适用于替换主机的名称、IP 和被替换主机的名称、IP 不一致的场景，也可用于将一个高性能的机器替换一个性能较差但其上实例状态正常的场景。实例修复操作会修复故障节点下的全部故障实例，实例修复过程中可能由于某些步骤出错导致失败，失败后需要使用相同的命令来重入修复过程，修复完成的实例会被成功拉起。

GaussDB 提供逻辑备份能力，可以将用户表的数据以通用的 text 或者 csv 格

式进行备份，并在同构/异构数据库中恢复该用户表的数据。逻辑备份采用分布式并行技术，并行地从每个数据实例 DN 中通过流式方式抽取待备份的用户表记录，提供了较高的备份恢复性能。

GaussDB 提供物理备份能力，可以将整个集群的数据以数据库内部格式备份到 OBS，并在同构数据库中恢复整个集群的数据。物理备份采用分布式并行技术，并行地对每个数据实例 DN 的数据文件进行物理备份，提供了极高的备份恢复性能。在基础之上，还提供压缩、流控、断点续备等高阶功能。

物理备份主要分为全量备份和增量备份，区别如下：全量备份包含备份时刻点上数据库的全量数据，耗时时间长（和数据库数据总量成正比），自身即可恢复出完整的数据库；增量备份只包含从指定时刻点之后的增量修改数据，耗时时间短（和增量数据成正比，和数据总量无关），但是必须要和全量备份数据一起才能恢复出完整的数据库。

典型的物理备份策略和应用场景如下：

- 周一，执行数据库全量备份。
- 周二，以周一全量备份为基准点，执行增量备份。
- 周三，以周二增量备份为基准点，执行增量备份。
- ...
- 周日，以周六增量备份为基准点，执行增量备份。

上述备份策略以一个星期为周期。

负载均衡为多 CN 提供一个统一的入口，将客户端的请求均匀的分发给各个 CN 服务器，使系统整体负载均衡。

负载均衡作为集群系统的一个重要组件，承担 2 个职责：

- 均衡各 CN 负载，充分利用多 CN 计算能力。
- 故障隔离，当 CN 故障后，负载均衡能感知故障，并自动停止向故障 CN 节点转发请求。故障感知的时间取决于不同的负载均衡模式，当在内网模式使用 JDBC client 做负载均衡时，CN 故障感知时间约为 30 秒，当在外网模式使用 ELB 做负载均衡时，故障感知时间默认为 3 秒(可配置)。

公共资源交易平台投标专用

GaussDB 支持 2 种模式的负载均衡：

- JDBC Driver 负载均衡

  用户只需在连接串中指定部分 CN，JDBC Driver 从这些 CN 中(高可用用途)获取所有可用的 CN 列表，然后在这些 CN 列表中进行负载均衡，当某个 CN 故障，将其从可用列表中剔除。刷新可用 CN 列表的时间默认为 10 秒(可配置)。建议用户在使用内网提供服务时使用该模式。JDBC Driver 负载均衡原理如所示。

- ELB 等第三方负载均衡

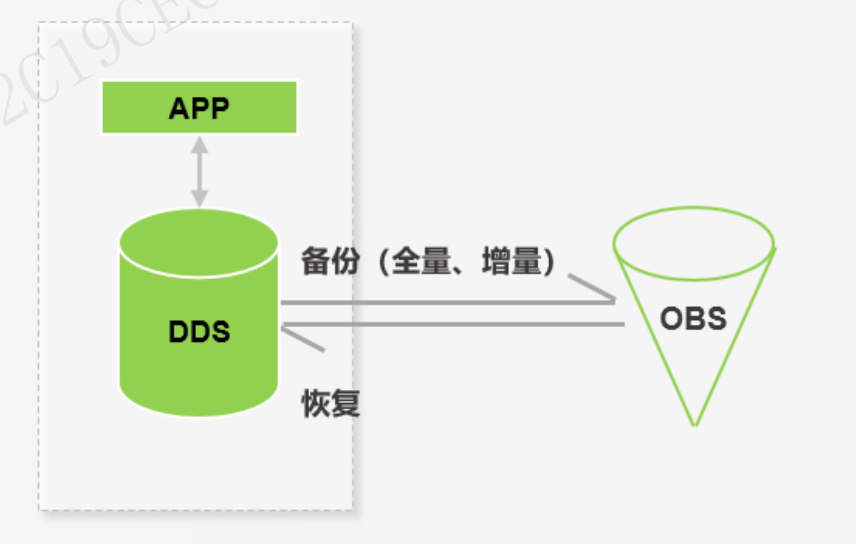
  GaussDB 支持对接 ELB 等第三方负载均衡方案，建议用户在使用外网提供服务时使用该模式，此时，JDBC Driver 的负载均衡功能可关闭。第三方负载均衡原理如所示。

3.2.3.1.6.6.7 分布式文档数据库

通过全量数据备份和周期性逻辑日志备份，当发生故障时可以保证能够回退到历史的任何版本。

- 物理数据备份：定期做全量数据备份，存放在 OBS 上；
- 副本集增量日志备份：每 5 分钟进行一次 oplog 日志备份；

图1-1 全量+增量数据备份



公共资源交易平台投标专用
AE2C19CEC17646E2A628BC88E14DB9

3.2.3.1.6.6.8 **国产数据库**

达梦数据库是一种功能丰富、高性能、可靠性强的关系型数据库管理系统，适用于各类企业级应用和大规模数据处理场景。它具备以下可靠性特点：

1. **架构稳定**：达梦数据库采用了先进的、经过时间考验的架构，确保其能够在各种复杂的企业环境中稳定运行。这种架构也允许数据库在高负载下维持高性能，不会因为数据量的增长或者并发请求的增加而降低性能。
2. **数据完整性保障**：达梦数据库提供了强大的数据完整性保障功能，通过事务管理、约束检查等机制，确保数据的准确性和一致性。即使在面临系统故障或者硬件故障的情况下，也能通过其恢复机制，保障数据的完整性不会受到损害。
3. **容灾与备份**：达梦数据库提供了全面的容灾和备份解决方案。无论是全量备份、增量备份，还是实时备份，都可以根据企业的实际需要来选择合适的备份策略。而且，一旦主数据库出现问题，备份数据库可以迅速接管，保证业务的连续性。
4. **安全性强**：达梦数据库对安全性有着极高的重视，提供了丰富的安全特性，包括数据加密、访问控制、安全审计等。通过这些安全特性，可以防止未经授权的访问，保护数据的机密性，确保只有合法的用户才能对数据进行操作。
5. **服务与支持**：达梦数据库拥有专业的技术支持团队和广泛的用户社区，可以提供全方位的服务和支持。无论是安装部署、性能优化，还是故障排查，都可以得到及时有效的帮助。
6. **数据一致性和完整性**：PostgreSQL提供了多种数据完整性检查和数据一致性保证机制。例如，它支持事务，确保数据的完整性和一致性在并发操作中得到保护。此外，PostgreSQL还提供了强大的约束和触发器功能，可以确保数据的一致性和完整性。
7. **备份和恢复**：PostgreSQL支持多种备份方式，包括物理备份和逻辑备份。物理备份方式如使用pg_dump进行全量备份，或使用pg_basebackup进行实时备份。逻辑备份方式如使用pg_dumpall进行全量备份，或使用

pg_dump进行部分备份。这些备份方式可以确保在发生故障时，数据能够快速恢复。

8. **高可用性**：PostgreSQL支持多种高可用性解决方案，如主从复制、流复制、逻辑复制等。这些解决方案可以确保在主节点发生故障时，从节点能够接管，保证服务的连续性。
9. **安全性**：PostgreSQL提供了强大的安全特性，包括访问控制、加密等。它支持SSL连接，可以保护数据在传输过程中的安全性。此外，PostgreSQL还支持多种身份验证方式，如密码认证、Kerberos认证等，确保只有授权用户才能访问数据库。
10. **监控和日志**：PostgreSQL提供了丰富的监控和日志功能，可以帮助管理员及时发现和解决问题。例如，它支持pg_stat_statements功能，可以监控SQL语句的执行情况；支持pg_stat_user_tables和pg_stat_user_functions功能，可以监控表和函数的执行情况。此外，PostgreSQL还支持日志记录功能，可以将操作记录到日志文件中，方便后续审计和分析。

大金仓数据库是一款基于国产技术、具备自主知识产权的高可靠性的数据库产品，广泛应用于金融、能源、政府等行业。

人大金仓数据库在可靠性方面具有以下特点：

1. **强大的容错能力**：KingbaseES数据库采用先进的容错技术，能够自动检测和处理各种故障，确保数据库的稳定性和可用性。即使在硬件故障或网络故障等情况下，也能够保证业务的连续性和数据的完整性。
2. **数据一致性保障**：KingbaseES数据库通过严格的事务管理和数据一致性保障机制，确保数据的完整性和一致性。它支持ACID事务，保证事务的原子性、一致性、隔离性和持久性，确保数据的准确性和可靠性。
3. **自动故障恢复机制**：KingbaseES数据库具备自动故障恢复机制，当发生故障时，系统会自动启动故障恢复流程，通过重做日志或撤销日志将数据恢复到一致状态。这种机制可以在短时间内恢复数据和系统状态，减少停机时间和影响。
4. **全面的数据备份和恢复功能**：KingbaseES数据库提供全面的数据备份和

公共资源交易平台投标专用

恢复功能，支持多种备份方式和恢复方式。它支持定时备份、增量备份、差异备份等多种备份方式，可以根据实际需求选择合适的备份策略。同时，它还支持多种恢复方式，如基于日志的恢复、基于数据的恢复等，可以根据实际需要选择合适的恢复策略。

5. **安全防护**：KingbaseES数据库具备完善的安全防护机制，通过身份认证、访问控制、数据加密等多种手段，确保数据库的安全性和机密性。它支持多种安全审计和日志记录功能，可以记录用户的操作和系统的状态，方便后续的审计和分析。此外，它还支持多种安全协议和标准，如SSL/TLS、Kerberos等，可以进一步提高数据库的安全性。
6. **性能优化**：KingbaseES数据库具备优秀的性能优化能力，可以通过调整参数、优化查询等方式提高数据库的性能和响应速度。它支持多种缓存技术、并行处理技术等，可以进一步提高数据库的性能和效率。此外，它还支持多种性能监控和调优工具，可以帮助管理员及时发现和解决问题。
7. **高可用性和扩展性**：KingbaseES数据库采用分布式架构设计，可以支持多个节点的高可用性和扩展性。它支持横向扩展和纵向扩展两种方式，可以根据实际需求选择合适的扩展方式。此外，它还支持多种负载均衡和流量控制技术，可以进一步提高系统的稳定性和可靠性。

南大数据库的可靠性主要体现在以下几个方面：

1. **多分片和多副本机制**：南大GBase 8a MPP Cluster采用分布式架构，数据被切分为多个分片并存储在不同节点上。每个分片都可以独立处理查询和更新操作，从而实现并行处理和负载均衡。同时，每个分片都提供多个副本数据冗余，当某个节点发生故障时，系统会自动切换至其副本数据节点进行工作，保证后续业务连续性。这种机制可以降低节点故障的木桶效应，提高系统的可用性和可靠性。
2. **自动切换机制**：南大GBase 8a MPP Cluster具备完善的自动切换机制，当某个节点发生故障时，系统会自动检测并切换至其副本数据节点进行工作。这种机制可以在故障发生时快速恢复数据和系统状态，保证业务的连续性。同时，系统还支持自动负载均衡和流量控制等功能，可以根

公共资源交易平台技术专用

据业务需求动态调整节点的负载和流量，保证系统的稳定性和可靠性。

3. **数据一致性和完整性：**南大GBase 8a MPP Cluster通过严格的事务管理和数据一致性保障机制，确保数据的完整性和一致性。即使在并发操作或分布式环境下，也能够保证数据的一致性和准确性。系统还支持多种数据复制和同步技术，如异步复制、同步复制等，可以根据业务需求选择合适的数据复制方式。
4. **安全防护：**南大GBase 8a MPP Cluster具备完善的安全防护机制，通过身份认证、访问控制、数据加密等多种手段，确保数据库的安全性和机密性。同时，它还支持多种安全审计和日志记录功能，可以记录用户的操作和系统的状态，方便后续的审计和分析。此外，系统还支持多种备份和恢复方式，如全量备份、增量备份、基于日志的恢复等，可以根据实际需要选择合适的备份和恢复策略。
5. **监控和告警：**南大GBase 8a MPP Cluster提供全面的监控和告警功能，可以帮助管理员及时发现和解决问题。系统可以监控节点的状态、负载情况、网络状况等指标，当出现异常情况时及时发出告警信息。此外，系统还支持多种监控工具和接口，如Prometheus、Grafana等，可以方便地进行自定义监控和告警策略设置。

3.2.3.1.6.7 **大数据高可靠**

华为MRS是一种高可靠性、高扩展性、高效性、高容错性、易运维的大数据管理和分析平台。作为一种新的数据平台，大数据系统存储了海量的业务数据，承载着企业的价值业务，数据的丢失、业务的中断，都会给企业带来有形、无形的损失，因此系统必须充分考虑业务连续性的要求，实现高可靠性。

3.2.3.1.6.7.1 **系统高可靠**

3.2.3.1.6.7.1.1　管理节点双机配置

3.2.3.1.6.7.1.2　异常场景下可靠保障

3.2.3.1.6.7.1.3　数据备份与恢复

3.2.3.1.6.7.2 **节点高可靠**

3.2.3.1.6.7.2.1　操作系统健康状态监控

3.2.3.1.6.7.2.2　进程健康状态监控

公共资源交易平台投标专用

3.2.3.1.6.7.2.3　硬盘故障的自动处理

3.2.3.1.6.7.2.4　节点RAID组的配置

3.2.3.1.6.7.3 **网络高可靠**

3.2.3.1.6.7.3.1　网络隔离

3.2.3.1.6.7.3.2　组网高可靠

3.2.3.1.6.7.4 **数据高可靠**

3.2.3.1.6.7.4.1　数据持久度

3.2.3.1.6.7.5 **集群可靠性**

3.2.3.1.6.7.5.1　支持AZ级高可靠

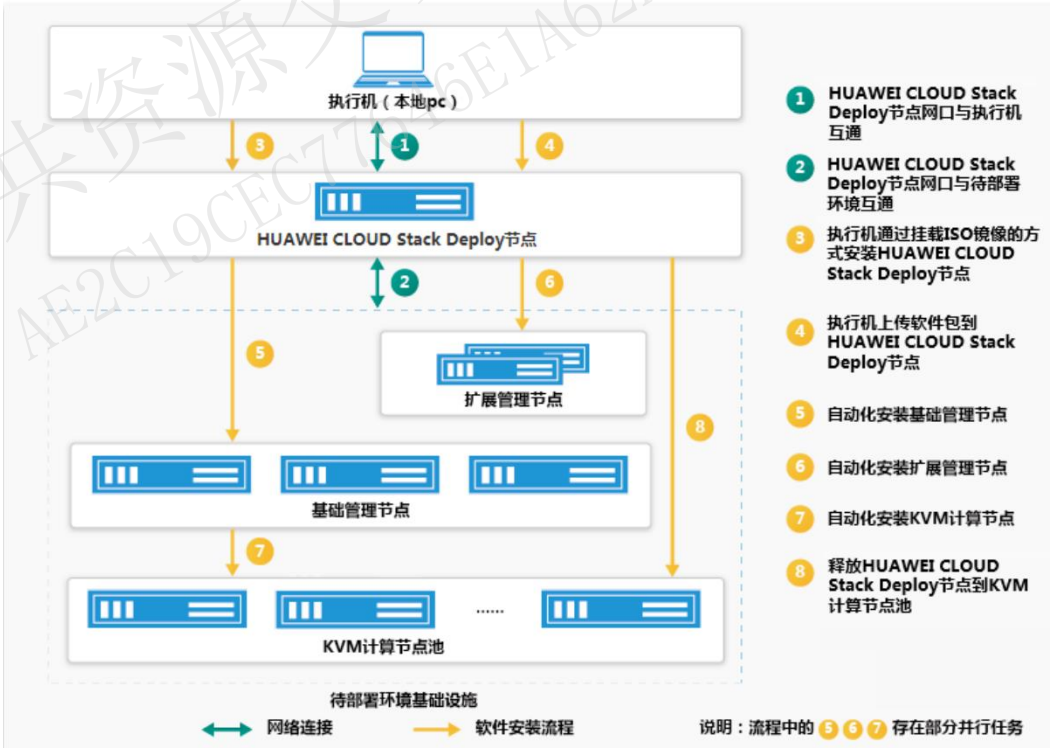
3.2.3.1.6.7.5.2　支持异地容灾

3.2.3.1.7　易用性建设方案

3.2.3.1.7.1 自动化安装

本项目提供自动化安装工具，实现对云平台的自动化安装部署管理。

HUAWEI CLOUD Stack Deploy 是华为云 Stack 自动化安装工具，端到端覆盖华为云 Stack 场景类型软件自动化部署和调测。



云平台安装部署

公共资源交易平台投标专用
AE2C19CEC7746E1A62A8BC8CFA14DB9

3.2.3.1.7.2 自动化升级

本项目提供自动化升级能力，实现不停机升级、远程升级等能力，为云平台提供持续的版本和云服务更新。

易操作

- 自动化：支持升级前一键式自动化局点信息搜集，基础服务&高阶服务自动升级前检查，以及升级checklist工具自动化
- 统一管理：支持升级密码统一管理
- 远程升级：支持远程升级，以及远程智能推包

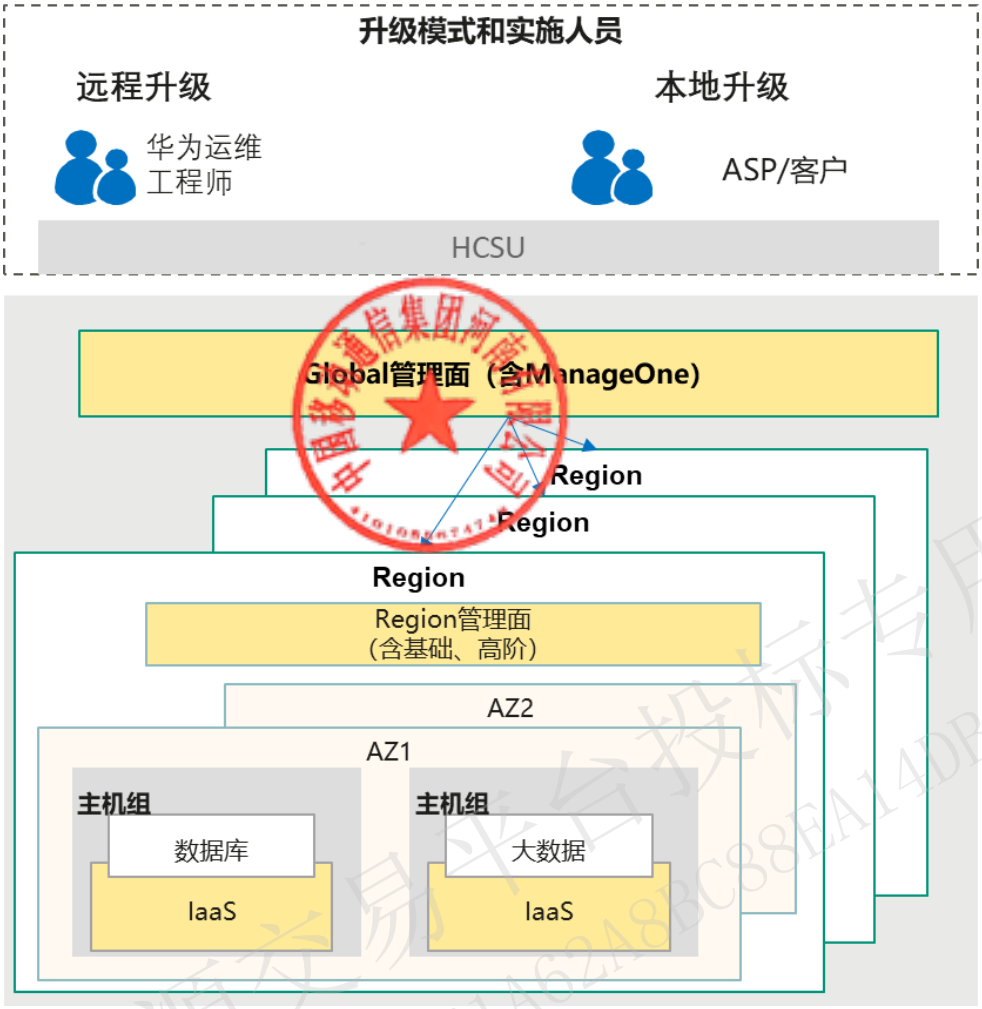
高效率

- 升级效率：基础服务&高阶服务全自动化升级；大规模场景（2K节点），管理面升级(网络单独1个时间窗除外）2个时间窗，计算节点业务面在线升级200节点/单个时间窗
- 单region高阶服务并行升级：支持单Region 10个高阶服务并行升级
- Region间解耦升级：融合部署，支持单region独立升级（除首region必须先升级），其他Region不需联动升级

高可靠

- 业务不中断：基础服务&高阶服务升级不中断业务
- 自动备份：升级前基础服务&高阶服务自动备份，防止升级出现重大问题时，可以进行重建
- 灰度升级：网元组件支持灰度升级（网元组件支持滚动升级、独立回退）；计算节点支持滚动升级；IaaS管理面滚动升级

公共资源交易平台投标专用



云平台升级能力

3.2.3.1.7.3 一体化运维平台

本项目提供统一的运维管理平台，如下图所示：

公共资源交易平台投标专用
AE2C19CFC17646F1A6248BC88EA14DB9



云运维平台

- 数据分析平台：打破数据孤岛，统一指标模型，基于分布式存储和流处理引擎，构建全局运维数据分析平台。
- CMDB配置管理平台：用来存储与管理企业IT架构中设备和系统的各种数据信息，依赖相关流程保证数据的准确、及时有效，实现信息共享，发挥配置信息的价值。
- AutoOps自动化平台：提供针对“原子”操作的编排能力以及任务执行的能力，能将原子操作编排为标准化的运维动作并按照不同的策略执行。
- 基于Agent和驱动对接技术，实现数据的全栈接入。
- 运维功能：支持集中监控、资源拓扑、日常运维、运维分析、系统管理等

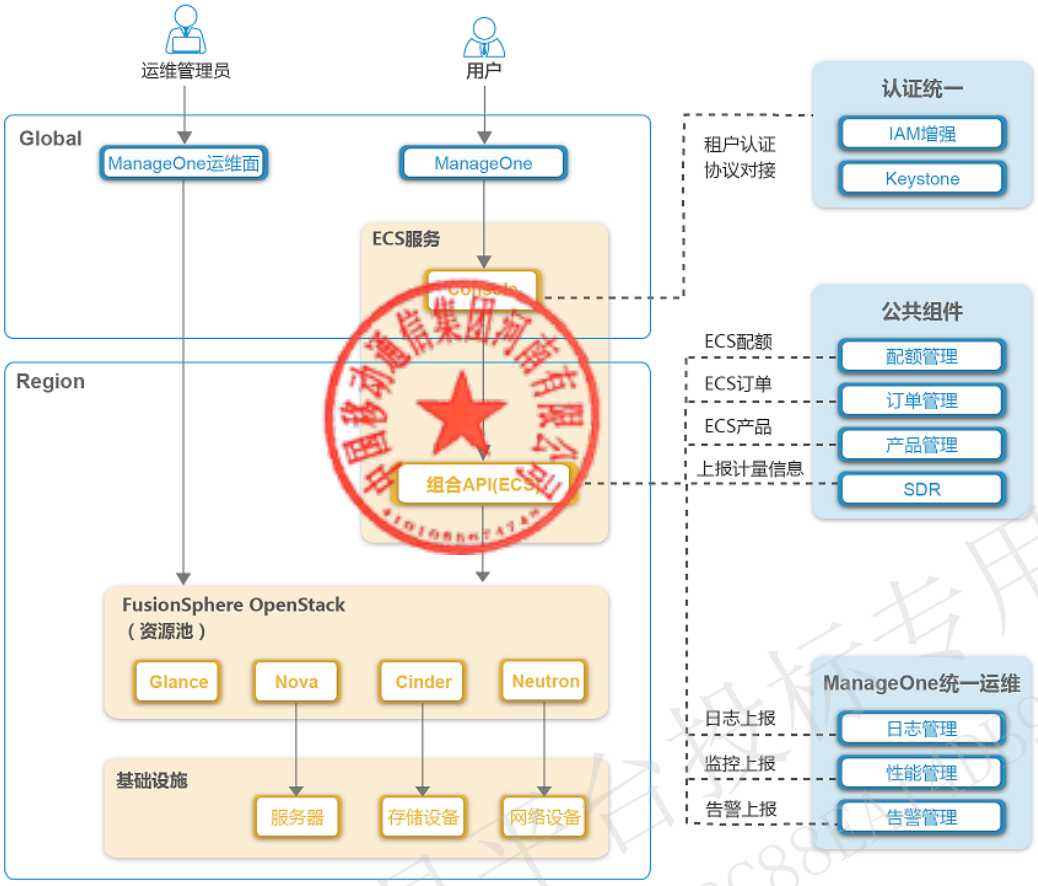
3.2.3.2 计算建设方案

3.2.3.2.1 弹性云主机服务

3.2.3.2.1.1 系统架构

ECS，即弹性云服务器，可以使用户可以在几分钟之内迅速地获得虚拟机设施，并且这些基础设施是弹性的，可以根据需求进行扩展和收缩。不同类型的弹性云服务器匹配不同的应用场景，可以根据自己的业务诉求选择相应的云服务器。

公共资源交易平台技术专用



弹性云服务器架构

组件类型	详情
Console	ECS_UI是以弹性云服务器为中心，对相关资源进行管理的Console控制台。
组合API(ECS)	组合API为弹性云服务器后台服务，可以理解为ECS_UI的服务端，支持调用FusionSphere OpenStack组件。ECS在前台发出的请求，经ECS_UI转发至组合API，组合API处理完后将结果返回ECS_UI。
资源池	Glance：提供镜像管理服务。 Nova：在OpenStack环境中管理计算实例的生命周期，包括批量创建，按需调度和停止。 Cinder：为运行的实例提供持久块存储。其可插拔驱动使创建和

组件类型	详情
	管理块存储设备更加便利。 Neutron：提供用于定义网络连通性和寻址的API。
认证统一	提供登录时的统一身份认证。
公共组件	由组合API上报ECS相关的配额、订单、产品信息、计量计费信息至ManageOne运营模块。
统一运维	由组合API上报ECS相关的日志、监控、告警信息至ManageOne运维模块。

ECS组件列表

3.2.3.2.1.2 服务能力

ECS 支持如下类型的云主机：

通用型

通用型弹性云服务器主要提供基本水平的 vCPU 性能、平衡的计算、内存和网络资源，同时可根据工作负载的需要实现性能的突增，具有短期发挥更高性能的能力。适用于那些不会经常（或始终不会）用尽 vCPU 性能，但会偶尔突然使用的场景，特别适合通用工作负载，如 Web 服务器、开发人员环境和小型数据库等，是很多应用程序的上好选择。

vGPU/GPU 加速型

可以用于深度学习、科学计算、CAE、3D 动画渲染、CAD 等高实时、高并发的海量计算场景，可在短时间内完成海量计算

通用独享型

提供性能稳定且资源独享的 CPU、内存运行环境，适用于对 CPU、内存性能有较高诉求 Web 服务、小型数据库运行环境。

内存优化型

内存优化型弹性云服务器基于 KVM 虚拟化平台，特别适合处理内存中的大型数据集。提供最大 512GB 基于 DDR4 的内存实例，是高内存计算应用的最佳选择。适用于对内存要求高，数据量大并且数据访问量大，同时要求快速的数据交

公共资源交易平台投标专用

换和处理的应用，适用于广告精准营销、电商、车联网等大数据分析场景。

超大内存型

超大内存型弹性云服务器内存要求高，数据量大并且数据访问量大，同时要求快速的数据交换和处理以及低延迟的存储资源。主要支持 OLAP 场景，如内存数据库、大数据处理引擎以及数据挖掘等应用。

ECS 服务通过 web 管理控制台，让用户自主的完成服务实例的申请、释放、变更等操作，从而灵活使用 ECS 服务。

- 支持多类型，多规格云服务器的选择和变更。
- 支持多类型云服务供选择，每种类型的弹性云服务器系统管理员可以根据业务需求自定义规格，建议项目中对业务VM规格进行分类和标准化，合理控制规格数量，中小规模项目建议规格不超过8种，大规模项目建议规格不超过16种。支持ECS服务实例的规格变更。
- 支持多种类型云硬盘供选择，例如分布式存储、SAN存储。
- 每个可用分区内可以选择对应的存储类型，包括分布式存储、SAN存储。可用分区内存储可以划分为多个不同能力的存储池，定义相应的Volume Type，例如可定义为普通IO、高IO、超高IO，供用户申请ECS服务时进行选择。
- 除系统盘之外，最大还可以支持挂载59块数据盘（最多支持59块SCSI盘，且SCSI盘和VBD盘的总数不能超过59，支持的VBD盘的总数参见表5-1），每块最大支持32T，满足用户不同的IO以及容量需求。
- 支持云硬盘的扩容，当磁盘空间不足时，可以通过扩容原有磁盘空间满足需求
- 网络自定义，自由划分子网、设置网络访问策略。：通过VPC（虚拟私有云服务）实现虚拟私有云网络管理，用户可自助规划VPC内网络的IP地址范围。为每个ECS实例提供私网IP和公网IP，用于不同的连接场景。私网IP可以内部连接使用，每个ECS实例支持同时挂载16张网卡（ARM场景下，可以挂载的网卡数目与ECS实例的磁盘设备类型和VBD磁盘数目相关，详细信息可以参考表5-1），每张网卡可以在不同的子网内，私网IP可以通过DHCP分配或指定IP地址；公网IP可以对外连接企业

内大网或互联网，可以根据需要申请绑定“EIP”为ECS实例申请公网IP。

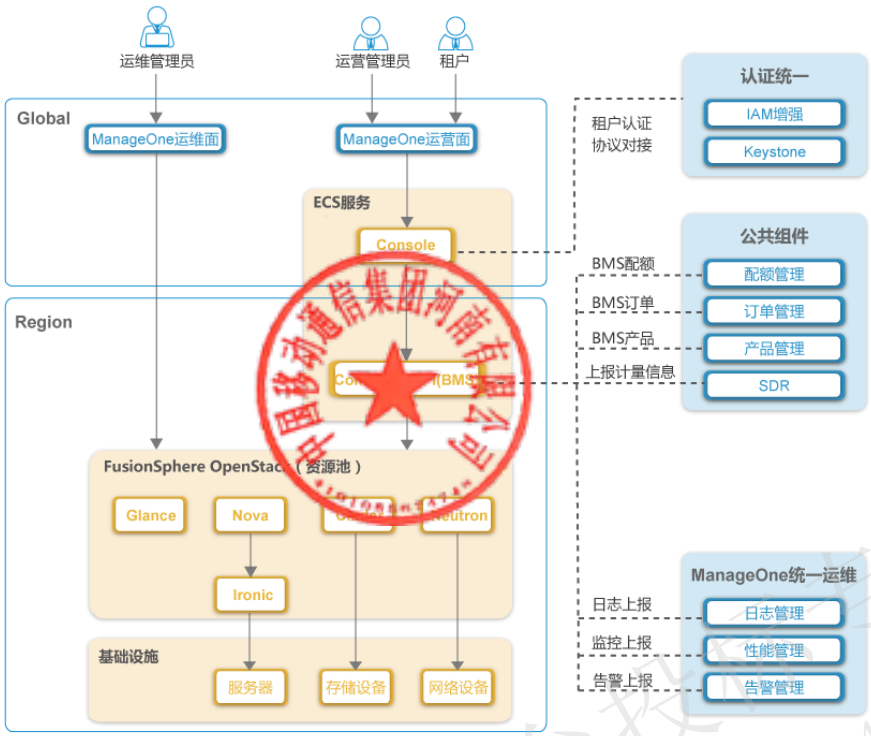
- 提供公共镜像能力和私有镜像服务，免安装快速部署操作系统与软件。
  - 公共镜像：公共镜像由系统管理员制作并注册到系统中，一般提供常见的标准操作系统镜像，所有用户可见。包含操作系统以及预装的公共应用。
  - 私有镜像：私有镜像服务用于满足用户个性化需求。选择私有镜像创建云主机，可以节省您重复配置云主机的时间。私有镜像仅用户自己可见。包含操作系统、预装的公共应用以及用户的私有应用。用户可基于ECS实例或者已有的镜像文件创建的私有镜像。
- 提供VNC控制台、远程终端和 API 等多种管理方式，满足用户多种登录需求，简化运维人员的工作难度，提升运维效率。
  - 用户可以完全控制自己创建的ECS实例。通过VNC控制台连接终端，解决系统问题，进行各项操作；也可以通过ECS服务控制台、API、命令行等类似工具对服务器进行启动、重启、关机等操作。
- 安全：支持用户申请时指定实例登录方式，ECS实例支持多种登录方式（密码、密钥对），密码防暴力破解，满足用户的登录安全需求。对于Windows的ECS实例，用户只能使用密码登陆。
- 支持云硬盘备份，在磁盘故障或数据错误时可快速恢复，使数据更加安全可靠。
- 实例反亲和性：支持在ECS控制台上创建一个或多个反亲和性组。在一个反亲和性组中的ECS实例将分配到不同的物理主机上来保证高可靠。用户可以把同一应用模块的ECS实例加入反亲和性组，增强应用的可靠性。

3.2.3.2.2 裸金属服务

3.2.3.2.2.1 系统架构

BMS 服务提供了一种裸金属服务器的使用形态，裸金属服务器上不运行虚拟化层，直接安装用户 OS。对于不适合 VM 部署的应用可以使用 BMS 服务，例如：数据库集群、OLAP 型应用（大数据、重载应用）。

公共资源交易平台投标专用



BMS系统架构

裸金属服务器组件详情：

组件类型	详情
Console	BMS服务前台portal界面，集成在ECS UI中。
Combined API (BMS)	BMS的服务端，集成在组合API中。组合API支持调用FusionSphere OpenStack组件。BMS在前台发出的请求，经ECS UI转发至组合API，组合API处理完后将结果返回ECS UI。
资源池	Ironic：在提供裸金属服务的分区内，部署在FusionSphere OpenStack的控制节点上。 Nova：在OpenStack环境中管理计算实例的生命周期，包括批量创建，按需调度和停止。 Cinder：为运行的实例提供持久块存储。其可插拔驱动使创建和管理块存储设备更加便利。 Neutron：提供用于定义网络连通性和寻址的API。 Glance：提供镜像管理服务。

公共资源交易平台技术应用
AE2C19CE6776461E1A62A8BC88EA14DB9

组件类型	详情
认证统一	提供登录时的统一身份认证。
公共组件	由组合API上报BMS相关的配额、订单、服务信息、计量计费信息至ManageOne运营模块。
统一运维	由组合API上报BMS相关的日志、监控、告警信息至ManageOne运维模块。

表 0-1 BMS组件列表

3.2.3.2.2.2 服务能力

通过裸金属服务器服务 web 管理控制台，用户可以自主完成服务实例的申请与释放，达到即开即用，用完归还的目标。

裸金属服务器服务（BMS）具有以下功能：

- BMS资源池可根据需要规划多种物理服务器规格（CPU、内存、硬盘）。用户可以根据不同场景的业务需求进行选择不同类型的物理服务器。
- BMS服务实例相对于裸金属服务器没有性能损失，专属于单个用户。 可以提供显着的计算性能和I / O吞吐量。
- 快速部署，BMS实例开通只需分钟级，满足用户的紧急需求。
- 支持云硬盘，除本地硬盘之外，最大还可以支持挂载60块云硬盘，满足用户不同的IO以及容量需求。
- BMS实例可以与ECS实例规划到同一个VPC(虚拟私有云网络)，用户可以方便的管理、配置内部网络；
- 为每个BMS实例提供公网IP和私网IP，用于不同的连接场景。公网IP可以对外连接互联网；私网IP可以内部连接使用，私网IP地址个数取决于物理服务器的网卡个数。
- 丰富的镜像，免安装快速部署操作系统与软件。
- 管理方便，用户可以通过Web页面或者开放API，同时管理一个、数百个、甚至数千个BMS实例。
- 支持裸金属服务器实例关键性能监控，以便快速发现定位主机故障。
- 完全控制，用户可以完全控制自己创建的BMS实例，拥有每个实例的管

公共资源交易平台投标专用

理员或者root用户访问权。

- BMS实例支持多种登录方式（密码、密钥），密码防暴力破解，满足用户的登录安全需求。对于Windows的BMS实例，用户只能使用密码登录，通过密钥发放实例时，操作系统会根据密钥生成随机密码，界面提供获取密码的功能。

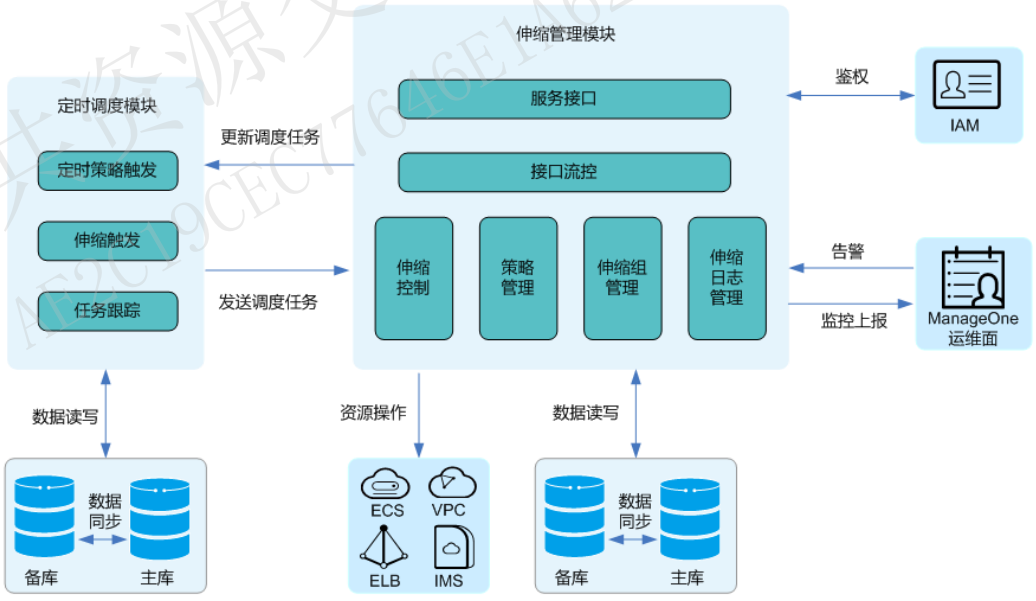
3.2.3.2.3 GPU 云主机服务

GPU 云主机服务属于弹性云服务下一种服务类型，可以用于深度学习、科学计算、CAE、3D 动画渲染、CAD 等高实时、高并发的海量计算场景，可在短时间内完成海量计算。

3.2.3.2.4 AS 弹性伸缩服务

3.2.3.2.4.1 系统架构

弹性伸缩服务是根据用户的业务需求和策略，自动调整其弹性计算资源的管理服务。弹性伸缩服务能够按照伸缩配置，在业务增长时能够实现自动增加实例数量，以满足业务需求；在业务下降时能够实现应用系统自动缩容，释放资源。



AS系统架构

弹性伸缩组件详情：

组件名称	详情
伸缩管理模块（部署在AS-SVR-SVR01和AS-SVR-SVR02虚拟机）	创建和管理弹性伸缩组，包括伸缩组内期望实例数、最小实例数和最大实例数的管理，伸缩组所属可用分区、VPC、子网及安全组，伸缩组的健康检查方式以及实例移除策略。 创建和管理伸缩配置，即根据对扩展的弹性云服务器的规格是否有特殊的要求，可通过使用新模板或已有弹性云服务器创建伸缩配置，使得伸缩组内弹性云服务器的规格均符合规格。 当伸缩配置不被任何弹性伸缩组使用时，可被删除。 创建和管理弹性伸缩策略，包括设置告警策略、定时策略和周期策略，启用、停止和删除伸缩策略。 控制伸缩活动，伸缩管理模块会在定时调度模块上配置的定时伸缩活动被触发或收到ManageOne反馈的告警后，从数据库中读取伸缩组及伸缩配置的详情，并对参数进行合法性校验，然后实时更新定时调度模块中的伸缩活动。
定时调度模块（部署在AS-SCHEDULE-SCHEDULE01和AS-SCHEDULE-SCHEDULE02虚拟机）	执行指标数据采集 执行健康检查 执行伸缩活动
数据库（主备）： 伸缩管理模块数据库（部署在AS-SVRDB-SVRDB01和AS-SVRDB-SVRDB02虚拟机） 定时调度模块数据库（部署在	伸缩管理模块数据库：存储伸缩组、伸缩配置和伸缩策略的配置信息。 定时调度模块数据库：存储任务信息。

公共资源交易平台投标专用

组件名称	详情
AS-SCHEDULEDB-SCHEDULEDB01和AS-SCHEDULEDB-SCHEDULEDB02虚拟机）	
弹性云服务器（ECS）	创建伸缩配置时，伸缩管理模块会去ECS校验伸缩配置参数。 伸缩组的健康检查方式为云服务器健康检查时，伸缩管理模块根据健康检查任务向ECS查询弹性云服务器健康状态。 伸缩活动触发时，伸缩管理模块会从数据库中读取伸缩组及伸缩配置的详情，并到ECS对其参数进行合法性校验。
镜像服务（IMS）	创建伸缩配置时，伸缩管理模块会去IMS校验伸缩配置参数。 伸缩活动触发时，伸缩管理模块会从数据库中读取伸缩组及伸缩配置的详情，并到IMS对其参数进行合法性校验。
虚拟私有云（VPC） 弹性负载均衡（ELB）	创建伸缩组，伸缩管理模块会去VPC校验伸缩组参数（VPC和网卡），还会去ELB校验伸缩组参数（监听器）。 伸缩活动触发时，伸缩管理模块会从数据库中读取伸缩组及伸缩配置的详情，并去VPC对其参数进行合法性校验，还需去ELB对其参数进行合法性校验。
ManageOne运维面	ManageOne会定时获取弹性伸缩组内各云服务器的监控数据，当获取的数据达到告警门限值，则发送告警给伸缩管理模块。

公共资源交易平台技术专用

组件名称	详情
统一身份认证（IAM）	具有用户身份管理和访问控制的功能。

AS组件列表

3.2.3.2.4.2 服务能力

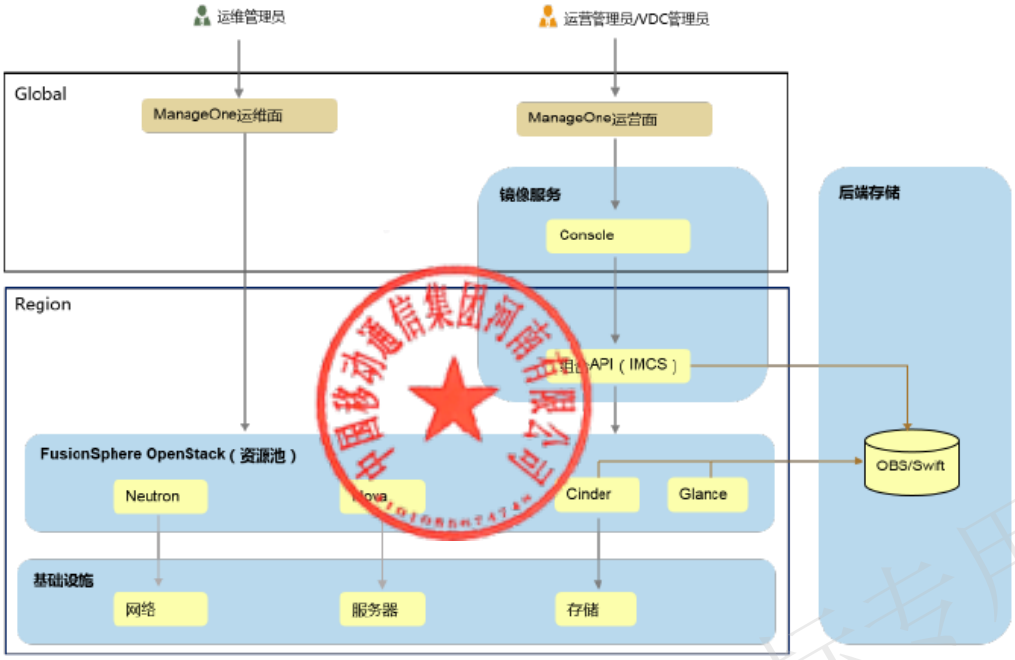
- 基于监控告警的动态触发模式：基于云监控性能指标（如CPU利用率、内存利用率、网络流入速率、网络流出速率），自动增加或减少ECS实例。
- 定时触发模式：配置一次性定时任务，定时地增加或减少ECS实例。
- 周期触发模式：配置周期性任务，周期性地增加或减少ECS实例，当周期性需求有所波动时，可同时配置告警触发模式以应付不可预期的变化。
- 支持期望实例数，最小实例数，最大实例数的管理；通过实例数范围控制，可以让您始终保持健康运行的ECS实例数量，自动替换不健康实例，以保证日常场景实时可用。
- 支持与ELB服务结合，自动为伸缩组虚拟机实例绑定负载均衡器。在增加或减少ECS实例时，自动向ELB实例添加或移除相应的ECS实例。
- 支持对伸缩组内的虚拟机进行健康检查，包括“云主机健康检查”、“负载均衡健康检查”，可以对不健康节点自动处理。

3.2.3.2.5 IMS 镜像服务

3.2.3.2.5.1 系统架构

镜像是虚拟机实例可选择的运行环境模板，一般包括操作系统和预装的软件(可包括公共应用软件以及用户私有应用软件)。镜像服务提供对公共镜像和私有镜像的自助管理能力，如下图所示。

公共资源入围单位投标专用



镜像服务架构

组件介绍：

层级	详情
Console层	以镜像服务为中心，对相关资源进行管理的Console控制台。
Service/API层	为镜像服务后台，可以理解为ECS UI(IMS)的服务端，支持调用FusionSphere OpenStack组件。IMS在前台发出的请求，经ECS UI(IMS)转发至组合API(IMS)，组合API(IMS)处理完后将结果返回ECS UI(IMS)。
资源池	Neutron：提供用于定义网络连通性和寻址的API。 Nova：在OpenStack环境中管理计算实例的生命周期，包括批量创建，按需调度和停止。 Cinder：为运行的实例提供持久块存储。其可插拔驱动使创建和管理块存储设备更加便利。可对接后端存储设备。 Glance：提供镜像管理服务。可对接后端存储。

公共资源交易平台投标专用
AE2C10CE27C46E1452A8BC88EA14DB9

层级	详情
基础设施	提供基本的网络、服务器和存储设备。
后端存储	可分为Swift后端存储和OBS后端存储，作为存储镜像文件的后端，便于后台调度和存储。

IMS组件列表

3.2.3.2.5.2 服务能力

镜像服务提供如下几种镜像类型：

公共镜像

公共镜像是云平台系统提供的标准镜像，包含常见的标准操作系统和预装的公共应用，能够提供简单方便的镜像自助管理功能，对所有用户可见。用户可以便捷的使用公共镜像创建弹性云服务器或裸金属服务器。

私有镜像

私有镜像是用户基于云服务器或外部镜像文件创建的个人镜像，仅用户自己可见，包含操作系统、预装的公共应用、用户的私有应用以及用户的业务数据。

- 系统盘镜像：系统盘镜像是用系统盘制作的镜像，包含操作系统、预装的公共应用及用户的私有应用。
- 数据盘镜像：数据盘镜像是只包含用户业务数据的镜像。
- 整机镜像：整机镜像是同时包含操作系统、预装的公共应用及用户的私有应用和用户业务数据的镜像。

可通过云服务器和外部镜像文件创建系统盘镜像、数据盘镜像和整机镜像。

通过已创建的系统盘镜像创建云服务器，可以节省您重复配置云服务器的时间。

通过已创建的数据盘镜像创建云硬盘，可以实现业务数据的灵活迁移，同时实现业务数据在多个弹性云服务器间共享。

通过已创建的整机镜像创建云服务器，可以快速实现整机迁移。

共享镜像

当用户需要将自己的私有镜像共享给其他用户使用时，可以使用镜像服务的

公共资源交易平台投标专用

共享功能。对于多资源集用户，共享镜像功能可以方便用户在同一个区域内的多个资源集间使用镜像。

当用户作为共享镜像的提供者时，可以共享指定镜像、取消共享镜像、添加或删除镜像的共享租户。当用户作为共享镜像的接受者时，可以选择接受或者拒绝其他用户提供的共享镜像，也可以移除已经接受的共享镜像。

3.2.3.3 存储建设方案

3.2.3.3.1 EVS 块存储服务

3.2.3.3.1.1 系统架构

EVS（Elastic Volume Service），即云硬盘，是一种虚拟块存储服务，主要为 ECS（Elastic Cloud Server）和 BMS（Bare Metal Server）提供块存储空间。用户可以在线创建云硬盘并挂载给实例，云硬盘的使用方式与传统服务器硬盘完全一致。同时，云硬盘具有更高的数据可靠性，更高的 I/O 吞吐能力和更加简单易用等特点，适用于文件系统、数据库或者其他需要块存储设备的系统软件或应用。

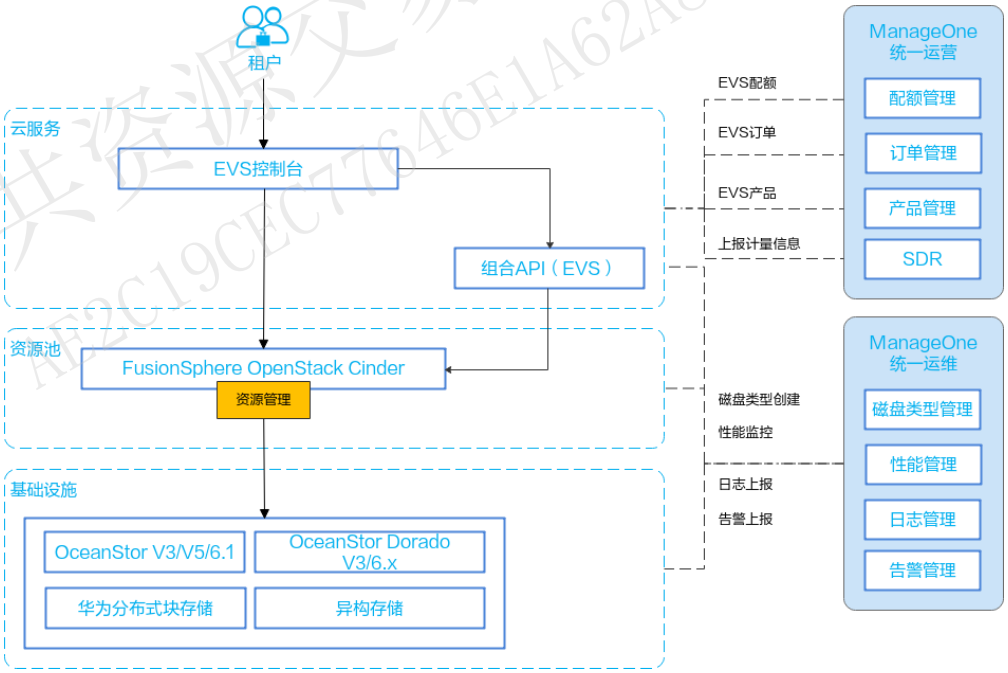


图 0-1 EVS系统架构

EVS 服务包括 EVS 控制台，EVS 服务 API，FusionSphere OpenStack Cinder 以及存储设备等组件。

公共资源交易平台技术专用

组件名称	详情
EVS控制台	EVS控制台对租户提供云硬盘服务入口，租户可通过控制台执行申请云硬盘等操作。
组合API（EVS）	EVS服务API在原生Cinder接口基础上封装或组合逻辑完成EVS服务部分功能，其接口可被EVS控制台或租户调用。
FusionSphere OpenStack Cinder	提供持久块存储，对块存储资源进行管理。在EVS服务里主要用于创建磁盘类型；在存储设备上创建磁盘，并将磁盘挂载给云服务器或裸金属服务器。
基础设施	物理存储设备，提供基于物理资源构建的块存储。可作为EVS服务后端存储的存储设备包括：华为SAN存储（OceanStor V3/V5/6.1，OceanStor Dorado V3/6.x），华为分布式块存储，异构存储（如HP 3PAR 8000系列）。
ManageOne统一运营	ManageOne统一运营为EVS服务提供配额管理，订单管理，服务管理，资源计量计费等功能。
ManageOne统一运维	ManageOne统一运维为EVS服务提供磁盘类型管理，性能监控，日志、告警等功能。

EVS组件列表

3.2.3.3.1.2 服务能力

云硬盘服务具有以下能力：

支持用户自助管理，包括创建、挂载、卸载、删除：

- 创建单个空白云硬盘：用户可以创建一块云硬盘。
- 基于已有快照创建云硬盘：申请云硬盘时，用户可以选择快照作为云硬盘的来源。
- 基于已有云硬盘创建云硬盘：申请云硬盘时，用户可以选择已有云硬盘作为云硬盘的来源。

公共资源交易平台授权专用

- 基于镜像创建系统盘：申请云硬盘时，用户可以选择镜像作为系统盘的来源。
- 基于镜像创建数据盘：申请云硬盘时，用户可以选择镜像作为数据盘的来源。
- 挂载云硬盘到云主机：用户可以将一块云硬盘挂载到某个弹性云服务器上。
- 从云主机卸载云硬盘：用户可以把一块已经挂载的云硬盘进行卸载。
- 删除单个云硬盘：用户可以删除一块云硬盘。

支持不同类型（例如：普通 IO、高 IO、超高 IO）的 EVS 磁盘，用户可以根据应用场景对 IO 的需求进行选择。

支持云硬盘快照管理：用户可以为云硬盘创建快照，提供云硬盘快照管理界面，展示快照列表，快照详细信息，支持删除快照、快照回滚到原云硬盘、从快照创建新云硬盘。

弹性扩容可以随时根据用户的需求扩展 EVS 磁盘的容量，满足不断增长的业务对更多存储容量的需求。

动态变更云硬盘的磁盘类型，在单套存储设备内的不同性能的 Pool 之间热迁移。

支持创建磁盘类型时，配置集中式存储的 SmartTier 和重删压缩特性，提供丰富的企业级增值特性。

单块 EVS 磁盘最大支持 64TB，最大限度满足用户对不同存储容量云硬盘的需求。

支持云硬盘 QoS 功能，支持对硬盘的带宽和 IOPS 限速。

云硬盘迁移，可以保证在不中断业务的前提下，在同一 AZ 内对云硬盘在存储阵列内或阵列间迁移，以精确匹配业务需求。

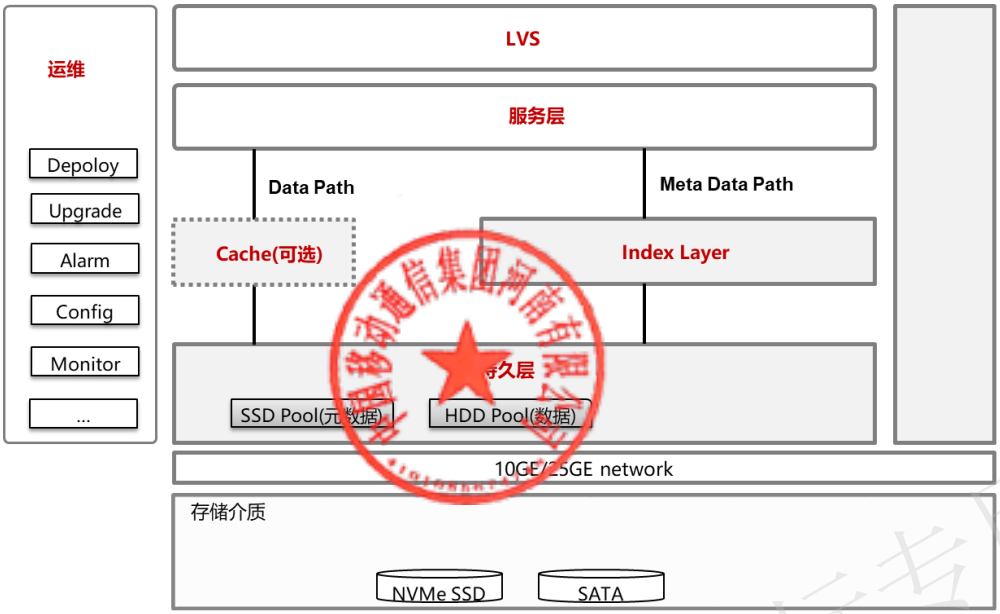
3.2.3.3.2 OBS 对象存储服务

3.2.3.3.2.1 系统架构

对象存储服务（Object Storage Service，OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠的数据存储能力，包括：创建、修改、删

公共资源交易平台投标专用

除桶，上传、下载、删除对象等。



OBS系统架构

如上图所示， OBS 从架构上主要分为三层：Persistence Layer（存储持久层），Index Layer（元数据服务层）和 Service Layer（对象语义服务层）：

Persistence Layer（存储持久层）基于通用服务器和介质构建统一的存储持久层，负责数据布局、负载均衡、数据恢复能力，提供 EC 数据冗余方式，可以灵活解决性能以及成本问题。可以看出，Persistence Layer 是 OBS 的基石，存储系统的扩展性、性能、可靠性均基于此。

Index Layer（元数据服务层）负责具体的元数据分布、索引、故障切换等，对上层的 Service Layer 提供高速的元数据存取和查询等能力，从上图中可以看到 Index Layer 的数据最终也是存储在 Persistence Layer，所以这些元数据一样共享底层 Persistence Layer 的数据存储能力，从而保证整个系统的所有数据都是高扩展、高可靠的。

Service Layer（对象语义服务层），提供 S3 协议的接口，负责对象业务的接入、全局统一命名空间等，同时具备完善的增值服务，比如桶加密、跨区域复制、QoS、多租户、配额等特性，业界通用的对象存储协议在 OBS 都可以提供，真正做到了按需使用，用户不用再为存储的选择而犯难。

3.2.3.3.2.2 服务能力

OBS 是一项面向 Internet 访问的服务，提供了基于 HTTP/HTTPS 协议的 Web

公共资源交易平台投标专用

服务接口，用户可以随时随地连接到 Internet 的电脑上，通过 OBS 管理控制台或各种 OBS 工具访问和管理存储在 OBS 中的数据。此外，OBS 支持 SDK 和 OBS API 接口，可使用户方便管理自己存储在 OBS 上的数据，以及开发多种类型的上层业务应用。

华为云 Stack OBS 是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。OBS 用户可以通过 ManageOne（运营中心）登录 OBS Console 进行基本的数据存储操作。用户在使用 OBS Console 服务的过程中，会通过 IAM 进行鉴权保证数据安全，下图运营中心服务的 IAM 负责帐户/用户/角色/AK/SK 信息分配，用户通过 AK/SK 访问 S3 服务时通过 IAM 做认证。OBS 对象存储服务还可以通过 S3 客户端、S3 SDK 进行访问。OBS 对象存储服务可以提供创建桶、删除桶、对象上传、下载、删除等操作。

- 支持创建、删除、查看桶。支持桶ACL设置、对象ACL设置和桶策略设置。
- 支持存储资源池在线扩展。
- 支持数据加密：通过KMS服务提供的密钥，对文件进行服务端加密。
- 支持数据检查：存储前一致性检查，确保存入数据是上传数据。
- 支持全局命名空间，无需指定区域即可访问全部桶和对象。
- 生命周期管理：用户可以为某个桶定义生命周期管理规则，来为该桶的对象定义各种生命周期规则。
- 支持查看桶配额（容量）。
- 支持最大48.8TB的超大文件存储，轻松搞定大数据存储。
- 多版本控制：开启多版本控制后。
  - 上传对象时，OBS自动为每个对象创建唯一的版本号。上传同名的对象将以不同的版本号同时保存在OBS中。
  - 可以指定版本号下载对象，不指定版本号默认下载最新的对象。
- 支持大文件分段上传和合并。
- 批量上传、删除对象。
- 支持桶日志管理：支持对桶的访问请求创建并保存访问日志信息，可用于请求分析或者日志审计。

公共资源交易平台投标专用

- 支持防盗链设置：为了防止用户在OBS的数据被其他人盗链，OBS支持基于 HTTP header中表头字段refer的防盗链方法。OBS同时支持访问白名单和访问黑名单的设置。
- 支持静态网站托管：OBS支持CORS规范，允许跨域请求访问OBS中的资源，通过CORS支持，使用JavaScript和HTML5来构建Web应用，直接访问OBS中的资源，而不再需要代理服务器做中转。 托管在不同域中的外部网页、样式表和HTML5应用，现在可以引用存储在OBS中的Web字体或图片，让这些资源能被多个网站共享。

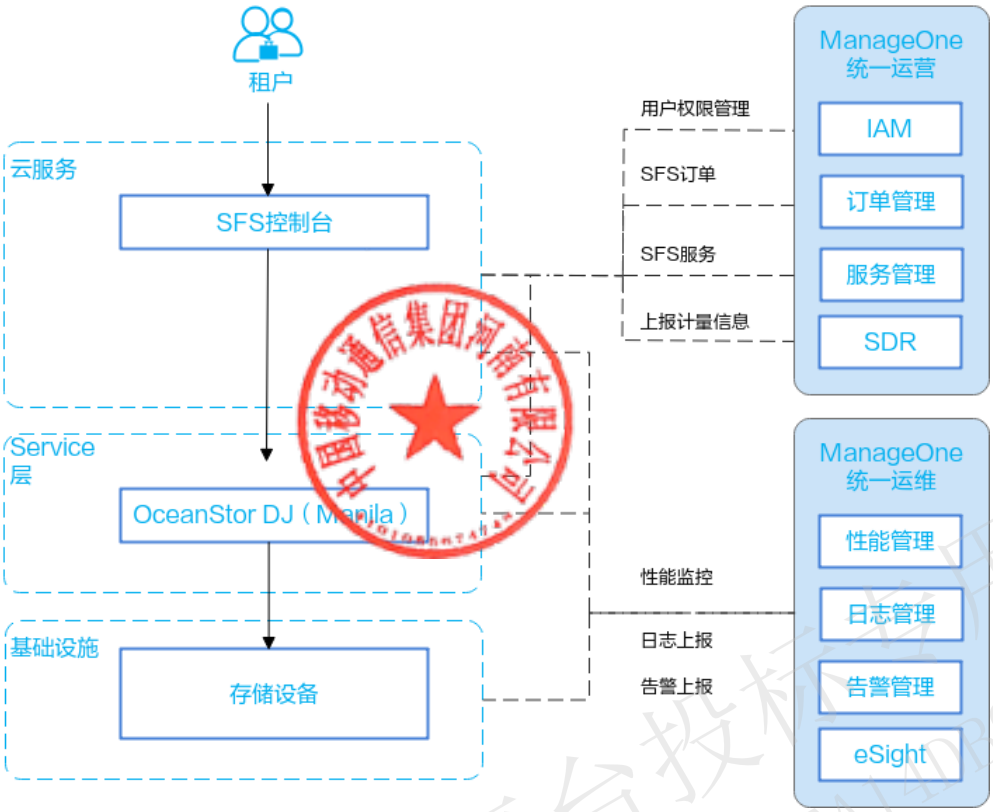
3.2.3.3.3 SFS 文件存储服务

3.2.3.3.3.1 系统架构

SFS（Scalable File Service），即弹性文件服务，为用户的弹性云服务器（ECS）提供一个按需扩展、弹性伸缩的高性能共享文件系统，符合标准文件协议（NFS 和 CIFS），能够弹性伸缩至 PB 规模，具备可扩展的性能，为海量数据、高带宽型应用提供有力支持。

华为云 Stack SFS 存储服务为用户提供了一个简单易用的文件存储服务门户，支持创建共享等服务。同时，文件存储服务也都能够通过后台 REST API 调用，方便用户把服务集成到自己的上层运维系统内。管理员可以在配置页面实现设备接入、租户配额设置等操作。

租户申请文件服务时，无需指定具体的存储设备，仅需选择管理员所创建的文件存储服务等级(SLA)。在收到服务请求后，在后台自动选择合适的存储设备，自动在设备上创建文件共享、自动完成网络配置、访问规则配置等一系列工作，使租户申请的文件存储服务立即可用。



SFS系统架构

SFS 服务包含以下组件并介绍如下：

组件类型	组件名称	详情
ManageOne 统一运营	IAM	为SFS提供身份识别和访问管理。
	订单管理	提供管理用户提交的订单的功能。
	服务管理	按照注册的云服务定义不同服务，提供统一服务管理。
	SDR	提供资源计量计费功能。
ManageOne 统一运维	性能管理	提供对基础设施的性能指标进行监控，及对监控数据进行分析的能力。
	日志管理	提供租户操作日志和运行日志的统一汇聚和查询功能。
	告警管理	提供告警数据接收、存储、集中监控查询及操

公共资源交易平台技术应用
AE2019CE7764E1A62A8BC88EA1AD39

组件类型	组件名称	详情
		作等功能，帮助运维人员根据告警信息快速排除故障。
	eSight	提供存储设备的性能监控和告警。
云服务	SFS控制台	提供SFS管理控制台。
	OceanStor DJ（Manila）	作为SFS服务端，接收SFS管理控制台请求。
基础设施	存储设备	文件存储设备，为SFS提供文件系统存储空间。支持OceanStor 9000、OceanStor Dorado 6.x

表 0-2 SFS组件列表

3.2.3.3.3.2 服务能力

功能点	功能点描述
存储兼容性	华为云 Stack SFS仅NFS共享支持OceanStor 9000 V300R006C20SPC300，CIFS和NFS同时支持，需要OceanStor 9000 V5 7.0.1版本才能支持。
支持创建文件存储	输入创建文件系统所需参数： 文件共享名称（非全局唯一，同一集群内不重复，批量创建加四位数字升序）、AZ、容量（可指定也可以无限制）、数量（>1就批量创建）、文件存储服务等级、协议（NFSv3、CIFS)、访问网络（SDN组网填虚拟私有云-VPC，无SDN，NFS填主机IP或IP段，CIFS填用户名称）
支持删除文件存储	文件存储删除后到回收站，回收站的文件存储可恢复和永久删除。回收站的文件存储不可挂载使用。冻结期的资源不可删除，但可以恢复。
查询文件共享	文件存储的详细信息，包括名称、ID、状态、可用

公共资源交易平台投标专用
AE2C19CE...

功能点	功能点描述
	分区、创建时间、挂载路径
修改挂载权限	无SDN组网，NFS支持添加或删除允许访问文件共享的主机IP地址，CIFS支持添加允许访问的用户或用户组名。 软件SDN和硬件SDN组网，支持添加允许访问文件共享的VPC网络，支持指定VPC网络中允许访问文件共享的主机IP，支持指定文件共享的用户权限。
文件存储容量调整	支持文件存储容量在线扩容/缩容（不限容量的文件存储不能扩容，不限容量的文件存储可缩容成限制容量，限制容量的文件存储可以扩容成不限制）
使用文件存储(手动挂载)	1.用户登录弹性云服务器，第一次挂载，在/etc/resolv.conf中添加域名解析DNS 2.使用showmount命令查看或者使用VDC业务员登录运营面portal，查看文件服务控制台中，所要挂载的文件存储的共享路径并复制 3.输入NFSv3的挂载命令，例如mount -t nfs -o vers=3 , timeo=600 , nolock xxxx.xxxx.xxx.com:/share-xxxx-xxx /mountdir，同时配置第5步 4.1输入命令后无报错，则进入挂载路径/mountdir，创建文件验证挂载成功 4.2输入命令后有报错，请提示信息进行问题修改 5.1弹性云服务器如需重启自动挂载文件存储，则修改/etc/fstab，增加mount命令开机自动挂载。 5.2步骤1-5.2，可以用本步骤实现，在OS中安装好文件服务自动挂载agent，在SFS用户页面上，选择文件共享的挂载标签，选择对应虚拟机agent会自动挂载文件共享。

公共资源交易平台技术专用
AE2C19CEC7761E1A6248B685A14DB3

功能点	功能点描述
使用文件存储（自动挂载）	1.用户的ECS虚拟机已经安装弹性文件服务自动挂载agent。 2.用户在弹性文件服务管理页面，点击弹性文件资源的挂载，选择需要挂载的ECS虚拟机。 3.用户也可以取消挂载弹性文件资源的挂载配置。
支持NFS协议	支持NFS V3协议
支持CIFS协议	支撑SMB2，SMB3协议
支持文件服务注册	支持定义无审批和有审批文件服务产品
租户DNS	提供租户访问SFS的域名解析能力
SFS云服务支持UI3.0	参考UI3.0规范
支持操作日志上报	日志包括（资源申请，变更，软删除，彻底删除，还原等）需要记录到MangeOne，云服务控制台操作也需要记录MangeOne
支持文件服务卸载	在安装时界面支持选择“取消注册到产品管理”
支持计量，计费	SFS按照话单格式生成话单文件，上传到ManageOne提供的SFTP服务器上
支持添加OceanStor 9000存储	支持接入存储设备（型号、IP、用户名、密码等）
文件存储设备删除	支持移除存储设备
创建/删除/修改文件存储服务等级	创建/删除/修改文件存储服务等级
支撑IPv6&IPv4双栈	支持IPv6的主机挂载共享，也支持IPv4的主机挂载共享。
华为云Stack Deploy部署	华为云Stack Deploy自动化安装部署SFS服务需要的组件，目前支持SFS-Console，SFS-manila的华为云Stack Deploy部署，不支持OceanStor 9000存储设备的华为云Stack Deploy部署。

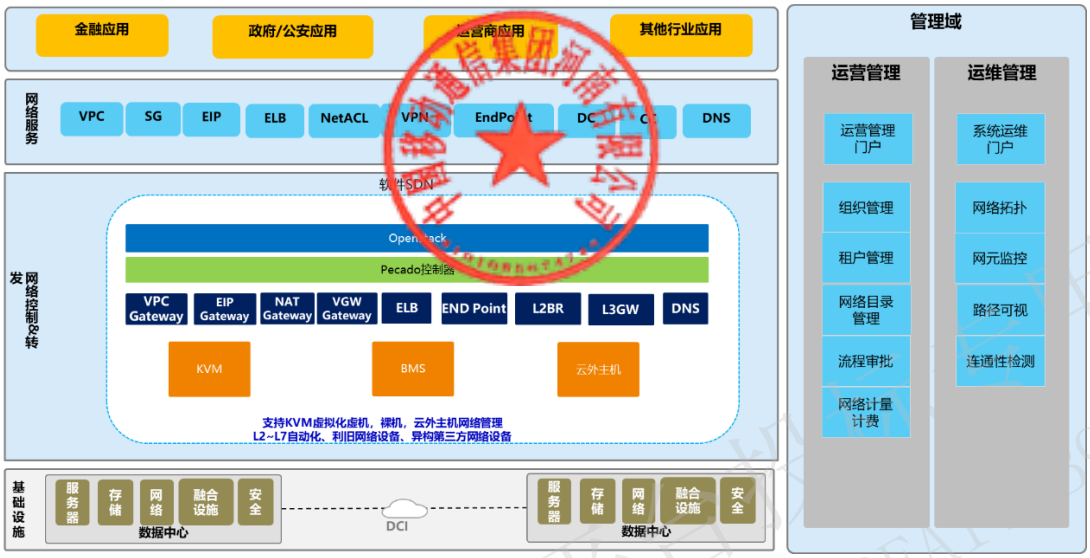
FS服务能力

公共资源交易平台投标专用

3.2.3.4 **网络建设方案**

3.2.3.4.1 SDN 网络系统架构

本项目提供 SDN 网络服务包，包含 VPC 服务、安全组、EIP、ELB、NetACL、VPN、VPC Endpoint，云专线 L3GW，二层专线 L2BR、DNS 等。如下图所示。



网路服务系统架构

- 云服务层

云服务层提供统一的云服务申请和自助操作服务控制台。

网络服务提供服务实例申请和自助操作维护控制台。服务分为 UI 和 Service 两部分，UI 提供面向用户的控制台 Service 提供服务管理功能。

- 网络控制&转发层

管理与控制能力由 Openstack、Pecado SDN 控制器 、计算节点 agent 来提供；

网络数据转发承载在 OVS、GW 之上。

- 基础设施层

服务器、存储、网络等物理基础设施，构成数据中心资源池的基础架构。

- 管理域

提供网络服务运营管理，运维监控能力。

3.2.3.4.2 ELB 弹性负载均衡服务

弹性负载均衡（Elastic Load Balance，简称 ELB）是将访问流量根据分配

策略分发到后端多台服务器的流量分发控制服务。弹性负载均衡可以通过流量分发扩展应用系统对外的服务能力，同时通过消除单点故障提升应用系统的可用性。

负载均衡为用户的应用请求提供负载分发的能力，用于将访问请求分担到用户多台虚拟机上，提高用户系统的业务处理能力；可保证访问请求能被转移到正常的虚拟机上，提高用户系统的可靠性。

虚拟负载均衡服务可为 HTTPS、HTTP、TCP、UDP、HTTP2(仅 HTTPS 协议支持)协议提供负载均衡。一个虚拟负载均衡下可以配置多个监听器，用户可以给不同业务申请不同的监听器。

负载均衡支持如下功能：

功能点	功能点描述
负载均衡管理	用户指定VPC创建ELB，可绑定的EIP支持公网访问
监听器管理	用户在已创建的ELB上管理监听器，包括名称，描述，负载均衡协议及端口，负载均衡算法，会话保持等，并同时创建健康检查
健康检查管理	用户为监听器配置健康检查，用于检查后端云主机的运行状态，包括健康检查协议，检查周期，超时时间，最大轮询次数等，与监听器创建合一； 支持修改健康检查类型，后端为HTTP的健康检查支持http和tcp类型可修改。 支持设置健康检查状态码，不设置默认为200 支持基于HTTP内容的深度健康检查，健康检查期望返回内容可以由用户设置，支持精确匹配和模糊匹配 支持基于TCP内容的深度健康检查，健康检查期望返回内容可以由用户设置，支持精确匹配和模糊匹配
Member管理	用户将后端云服务器/物理机添加到指定的监听器后面，可设置Member的权重
七层基础转发策略管理	7层流量按照HTTP头部内容(域名和URL)转发到不同的后端云服务器/物理机。对转发规则和策略进行管理和操作

公共资源交易平台技术专用

功能点	功能点描述
七层高级转发策略管理	高级转发策略开启后，ELB实例会根据用户配置的高级转发策略将不同的请求按照不同的方式处理，大致过程如下 客户端发送请求至ELB； ELB首先根据事先设置好的高级转发策略中的转发规则匹配请求； ELB再根据转发规则对应的动作将客户端请求转发至对应的后端服务器进行处理； 最后由后端服务器返回响应至客户端。 每条高级转发策略必须包含转发规则和动作。 支持的转发规则有：域名、URL、多URL或者多域名的组合。 支持的动作类型有：转发至后端服务器组、重定向至监听器、重定向至URL。
白名单管理	对访问ELB的客户端IP进行安全控制，只有允许的IP能通过ELB访问后端云服务器/物理机
证书管理	为ELB服务的HTTPS证书卸载功能提供的证书管理功能，包括证书查询，创建，删除
支持轮询/最少连接/源IP	支持加权轮询、加权最小连接和源IP算法。
支持HTTP重定向	将HTTP访问重定向至HTTPS，客户端HTTP的访问请求，后端服务器返回HTTPS的响应。
支持按弹性负载均衡粒度监控性能指标	云平台提供的云监控服务，可以对弹性负载均衡器的运行状态进行日常监控。您可以通过管理控制台，直接查看弹性负载均衡器的各项监控指标。
支持标准OpenStack API	可以通过标准OpenStack API接口调用负载均衡的API完成相关的操作，兼容性强。
支持会话保持	会话保持功能可以识别客户与服务器之间交互过程的

公共资源交易平台技标专用

功能点	功能点描述
	关联性，在作负载均衡的同时，还保证一系列相关联的访问请求会保持分配到同一台服务器上。
基于ELB实例的限速	ELB实例限速指标包括 并发连接数：该ELB实例总连接数，单位是个 新建连接数：单位时间支持的最大新建连接个数。单位是个/秒 查询会话数：针对七层负载均衡单位时间最大访问速率，单位是qps 带宽：该ELB实例总的访问带宽，单位是Mbit/s
监听器空闲超时	ELB监听器空闲超时指标包括 TCP空闲超时时间：四层负载均衡是client到后端真实服务器的TCP连接空闲超时时间，取值范围0~4000秒；七层负载均衡是client到elb的TCP连接空闲超时时间；取值范围300~4000秒 HTTP请求超时时间：Client http请求elb超时时间。取值范围1~300秒 HTTP响应超时时间：后端真实服务器响应elb http请求超时时间。取值范围1~300秒
支持国密算法和证书	支持《GM/T 0024-2014: SSL VPN技术规范》定义的ECDHE-SM4-SM3、ECC-SM4-SM3算法套件。 支持国密证书（签名证书、加密证书）
支持混合负载均衡	混合负载均衡的后端服务器组不仅支持添加云上VPC内的服务器实例，还支持以Target IP地址形式添加。可以是本VPC IP、其他VPC IP、其他Region IP、云下数据中心的服务器IP。帮助用户根据业务诉求灵活配置，将流量请求转发到云上、云间或云下的服务器上 ELB访问后端member场景包括： 通过VPC Peering访问

公共资源交易平台投标专用

功能点	功能点描述
	通过云连接访问 通过基础型云专线或Peering的云专线访问 通过VPN或Peering的VPN访问 通过L2BR或Peer的L2BR访问 通过L3CW或Peer的L3CW访问

ELB 特性列表

3.2.3.4.3 EIP 弹性 IP 服务

弹性 IP（EIP, Elastic IP Address），是可以独立购买和持有的公网 IP 地址资源，通过绑定 EIP 到云上的资源，云上的资源就可以与 Internet 上的资源进行通信。

EIP 是一种 NAT IP。通过 NAT 方式映射到了被绑定实例上。因此，绑定了 EIP 的实例可以直接使用这个 IP 进行公网通信，但是在实例上并不能看到这个 IP 地址。

初始情况下，您没有申请任何 EIP，如果需要使用 EIP，需要申请。EIP 一次只能绑定到一个云上的资源实例，但是解绑之后，该地址不会被释放，你可以继续把这个 EIP 绑定到其它云上的资源实例。释放 EIP 之后，该地址会被回收，您不能再使用。

- 一个实例接口只能绑定一个EIP。
- 一个EIP只能绑定到一个实例接口。
- 可以将EIP从一个实例解绑，再绑定到另外一个实例。
- EIP绑定和解绑不影响实例的运行。
- EIP绑定和解绑实时生效。
- EIP到期后不能绑定给云实例使用。
- ECS和BMS有多个网卡的时候，每个网卡都可以绑定EIP，默认主网卡的EIP可以访问，如果需要通过非主网卡的EIP访问，需要改ECS或者BMS的默认网关为非主网卡网关。
- EIP支持独享带宽和共享带宽两种限速功能。默认限速最大值300M，最小值1M。

功能点	功能点描述
支持指定EIP网络和子网创建EIP	创建EIP
支持指定EIP地址和系统自动分配	可以指定IP地址创建EIP，如果指定的IP没有被分配出去，可以创建成功。 也可以让系统自动分配EIP
支持批创多个EIP	批量创建多个EIP
支持指定EIP时长	设置EIP的有效时长，最小单位是天，也可以不限时长
支持EIP到期后延期	EIP到期后，并不会释放，可以延期
支持EIP释放	EIP释放后，被系统回收
支持绑定EIP给ECS，BMS，虚IP，ELB	绑定EIP给ECS，BMS，ELB和虚IP，这些对象就可以通过公网访问
支持解绑EIP	把EIP从解绑后，可以再绑定给其它ECS，BMS，ELB和虚IP使用
EIP带宽限速	限制EIP的带宽，支持独享带宽和共享带宽。 共享带宽多个EIP公用指定的共享带宽。

EIP特性列表

3.2.3.4.4 VPC 虚拟私有云服务

VPC 全称虚拟私有云（Virtual Private Cloud），用于构建隔离的、用户自主配置和管理的虚拟网络环境，提升云资源的安全性，简化用户的网络部署。VPC 支持以下特性：

子网服务

子网服务用于二层广播隔离（一个子网是一个广播域），一个 VPC 内可以包含一个或者多个子网。一个子网可以包含一个 IPv4 的地址块和一个 IPv6 的地址块。

项目级子网

项目级子网是通过子网提供与其他网络隔离的、可以独享的网络资源，仅加入到该子网的虚拟机才能访问该网络上的资源。项目级子网仅有二层能力，无外

公共资源交易平台投标专用

部网络出口。

虚拟 IP 服务

虚拟 IP（即 VIP）是一个未分配给真实弹性云服务器网卡的 IP 地址，可以同时绑定多个虚拟机网卡。主要用在弹性云服务器的主备切换，达到高可靠性 HA（High Availability）的目的。

端口 Qos 服务

端口 QoS 特性提供虚拟网卡的流量整形控制。

SNAT 服务

SNAT(Source Network Address Translation)，即源地址转换，将 VPC 内的一段网段内的 IP 地址映射成为弹性 IP 地址。

DNAT 服务

DNAT(Destination Network Address Translation)，即目的地址转换，将公网 IP 映射给 VPC 内云主机使用，使云主机对外提供服务。一个公网 IP 可以给多个 VM 的不同 Port 使用。

公共服务访问服务

租户虚机可以直接访问云平台公共服务。

专线/路由直通服务

专线/路由直通服务提供 VPC 子网和云外子网三层直接互访的能力，不需要做地址转换。

VIP 服务

虚拟 IP 主要用在云服务器的主备切换，达到高可靠性 HA(High Availability)的目的。多个主备部署的弹性云服务器可以在绑定虚拟 IP 地址时选择同一个虚拟 IP 地址。用户可以为该虚拟 IP 地址绑定一个弹性公网 IP 地址，这样从互联网也可以访问后端绑定了同一个虚拟 IP 地址的多个主备部署的弹性云服务器，增强容灾性能。需要注意的是用户绑定的多个弹性云服务器自身要能提供类似 keepalive 的动态配置虚拟 ip 的能力。

对等连接

对等连接是指两个 VPC 之间的网络连接。用户可以使用私有 IP 地址在两个 VPC 之间进行通信，就像两个 VPC 在同一个网络中一样。同一区域内，您可以在

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB5

自己的 VPC 之间创建对等连接，也可以在自己的 VPC 与其他租户的 VPC 之间创建对等连接。

VPC 组播

VPC 组播是一项 VPC 扩展能力的高级网络功能，旨在混合云平台上可支持组播能力，针对传统业务上云，必须要使用组播能力的场景，提供云内二层、三层组播能力，提供组播源、点播者在云内、云外等多种位置的场景组合，几乎覆盖传统环境中组播的所有场景，保证客户应用无改造上云。

VPC 流日志

VPC 流日志功能，是通过记录虚拟私有云中流量信息，帮助您检查及优化安全组和网络 ACL 控制规则、监控网络流量以及进行网络攻击分析。依赖高阶服务 AOM LTS 提供的日志持久化、搜索等功能。

路由表管理

路由表由一系列路由规则组成，用于控制虚拟私有云内子网的出流量走向。VPC 中的每个子网都必须关联一个路由表，一个子网一次只能关联一个路由表，但一个路由表可以关联多个子网。

3.2.3.4.5 云专线服务

云专线（Direct Connect）用于搭建用户本地数据中心与华为云 VPC 之间高速、低时延、稳定安全的专属连接通道，充分利用华为云服务优势的同时，继续使用现有的 IT 设施，实现灵活一体、可伸缩的混合计算环境。

云专线提供云上子网和云外子网直接路由互访，不需要做地址转换，网络带宽时延有保障，配置和维护简单。

基础型云专线——vRouter 集群作为专线网关，需要事先手动打通 vRouter 与云外 PE 之间的 vlan 通道。路由发布支持静态路由方式。基础型云专线服务不依赖硬件设备，部署灵活，易于扩容。

增强型云专线——需要一对华为硬件交换机作为专线网关，支持特定组网的配置自动化下发，也支持客户手动配置出口已满足特殊组网需求。路由发布模式支持静态路由和 BGP 动态路由两种方式。增强型云专线依赖华为特定型号交换机，但流量不经过软件网元，转发性能高。同时，增强型云专线针对特定组网自动化程度高。

公共资源交易平台投标专用

3.2.3.4.6 VPC Endpoint 终端节点服务

VPC 终端节点（VPC Endpoint），可以将 VPC 私密地连接到终端节点服务（云服务、用户私有服务），使 VPC 中的云资源无需弹性公网 IP 就能够访问终端节点服务。

VPC 终端节点提供“终端节点服务”和“终端节点”两种资源。

- 终端节点服务：指将云服务、用户私有服务配置为VPC终端节点支持的服务，即终端节点服务。
- 终端节点：在VPC和终端节点服务之间提供连接通道。租户在VPC中创建自己的应用程序并将其配置为终端节点服务，同一区域下的其他VPC可以通过创建在自己VPC内的终端节点访问终端节点服务。

3.2.3.4.7 L2BR 二层桥接服务

二层桥接服务（L2 Bridging）提供了云外网络与云内 VPC 子网二层互通的能力，用来满足客户业务迁移上云 IP 地址不变、客户同一业务云内云外部署二层互通等场景。

二层桥接支持云内云外二层互通，使用 CE 交换机作为网关（L2BR），用户数据包在计算节点直接走 VxLan 隧道到 L2BR，L2BR 再将 VxLan 报文转换为 vlan 报文发送给云外 PE 设备，整个路径不经过软件网元。

租户可以在 VPC Console 上基于 L2BR 接入点创建 L2BR 实例。基于同一个 L2BR 接入点创建的 L2BR 实例与云外 PE 连接的 vlan 不能重叠。基于不同 L2BR 接入点创建的 L2BR 实例与云外 PE 连接的 vlan 可以重叠。同一个子网只能创建 1 个 L2BR 实例。

- 支持通过L2BR实现传统VLAN网络和数据中心的VPC二层和三层互通。
- 支持通过L2BR实现传统VLAN网络使用数据中心内的ELB、云专线、VPN、VPC Peering服务、Endpoint服务
- 支持通过L2BR扩展支持组播能力

3.2.3.4.8 NAT 网关云服务

NAT 网关，NAT 网关（NAT Gateway）能够为虚拟私有云内的云主机（弹性云

服务器、裸金属服务器），提供网络地址转换服务，使多个云主机可以共享弹性公网 IP 访问 Internet 或使云主机提供互联网服务。

NAT 网关分为 SNAT 和 DNAT 两个功能。

SNAT 功能通过绑定弹性公网 IP，实现私有 IP 向公有 IP 的转换，可实现 VPC 内多个云主机共享弹性公网 IP，安全，高效的访问互联网。

DNAT 功能绑定弹性公网 IP，可通过 IP 映射或端口映射两种方式，实现 VPC 内多个云主机共享弹性公网 IP，为互联网提供服务。

3.2.3.4.9 vFW 网络 ACL 服务

网络 ACL 用于子网级别的安全防护：网络 ACL 是一个或多个子网的访问控制策略，根据与子网关联的入站/出站规则，判断数据包是否允许流入/流出关联子网。规则匹配的顺序和配置顺序一致。

网络 ACL 服务的功能如下：

- 规则匹配域支持：源端口，源IP地址，目的端口，目的IP地址，协议；
- 一条规则匹配域中源端口/目的端口支持多个，源IP地址/目的IP地址支持多个
- 可以调整规则的顺序；
- 协议支持：TCP，UDP，ICMP，ANY；
- 动作支持：Allow， Deny，Reject；
- REJECT动作会返回一个拒绝(终止)数据包(TCP FIN或UDP-ICMP-PORT-UNREACHABLE)，明确的拒绝对方的连接动作。
- Deny动作只是简单的直接丢弃数据，并不反馈任何回应。需要Client等待超时，Client容易发现自己被防火墙所阻挡。
- 网络ACL实例支持与子网绑定，一个网络ACL实例支持和多个子网绑定，一个子网不能同时加入两个网络ACL实例；
- 支持入方向和出方向流量防护；

网络 ACL 是分布式的，既可以做东西向流量的安全防护，也可以做南北向流量的安全防护。

功能点	功能点描述
支持创建和删除ACL实例	创建ACL实例

公共资源交易平台投标专用

功能点	功能点描述
支持设置ACL实例时长	设置ACL实例的有效时间，到期后，不能操作ACL实例，也可以不限时间
支持ACL实例延期	延长ACL实例有效时间
支持关闭ACL实例	关闭ACL实例后，规则不生效
支持添加/删除/修改ACL实例入方向规则	配置入方向规则，设置匹配条件
支持添加/删除/修改ACL实例出方向规则	配置出方向规则，设置匹配条件
支持调整规则顺序	可以在现有规则前后插入新的规则，用于调整规则顺序
支持关联ACL实例/取消关联到子网	把ACL实例作用到子网上

网络ACL特性列表

3.2.3.4.10 SG 安全组服务

安全组控制云主机网络消息的流入流出，支持白名单能力。当云主机申请成功后，可以将云主机加入到某个安全组内，安全组上配置安全规则。

安全组是一组对虚拟机的访问规则的集合，为同一个 VPC 内具有相同安全保护需求并相互信任的虚拟机提供访问策略。安全组用来实现组内和组间的访问控制，加强虚拟机的安全保护，实现 VPC 内部的网络隔离。

系统存在一个默认安全组(default)，当项目管理员创建虚机不指定安全组的时候，系统会自动分配默认的安全组。

参数	描述
协议	支持限制某类型协议的消息流入流出，协议类型：TCP、UDP、ICMP、Any。
方向	设置网络消息的流入流出方向。
源	控制哪些IP地址或授权指定安全组可以访问安全组内的云主机。源IP范围可以通过子网、IP段。
端口	对于TCP、UDP协议，可以设置端口范围。

参数	描述
优先级	安全组规则优先级

SG特性列表

3.2.3.4.11 VPN 服务

VPN(Virtual Private Network)，即虚拟私有网络，提供端到端的私有访问通道。

IPSec VPN（Internet Protocol Security Virtual Private Network）业务用于在公用网络上，为远端用户和 VPC（Virtual Private Cloud）之间建立一条安全加密的通信隧道，使远端用户通过 IPSec VPN 直接访问 VPC 中路由网络内的业务资源。

功能点	功能点描述	功能实现约束（含组合约束）
VPN管理	IPSec VPN管理，配置VPN名字，指定IP或自动方式分配VPN网关公网IP地址，配置对端地址和两端子网，配置VPN加密算法、认证算法、传输协议等	单VPC内的所有VPN使用相同的VPN网关公网IP地址
VPN限速	对VPC通过VPN隧道访问用户自有数据中心的出口流量进行带宽控制。	仅TypeI支持，TypeII不支持。
自定义路由	VPN业务根据自定义路由转发	仅TypeI支持。 自定义路由下一跳不支持云外IP。
支持国密算法和证书认证	支持《GB/T 36968-2018 信息安全技术IPSec VPN技术规范》： 支持IKEv1国密证书认证 支持国家标准算法	通用标准算法： IKE/IPSec加密算法：AES-128、AES-192、AES-256 IKE/IPSec认证算法：SHA-256、SHA-384、SHA-512

功能点	功能点描述	功能实现约束（含组合约束）
	支持证书管理	IKE非对称加密算法：RSA 国家标准算法： IKE/IPSec加密算法：SM4 IKE/IPSec认证算法：SM3 IKE非对称加密算法：SM2

VPN特性列表

同时本项目将在边界墙上配置 SSL VPN 功能，SSL VPN 是以 SSL 协议为安全基础的 VPN 远程接入技术，移动办公人员（在 SSL VPN 中被称为远程用户）使用 SSL VPN 可以安全、方便的接入 VPC 内网，访问企业内网资源，提高工作效率。

边界防火墙向远程用户提供 SSL VPN 接入服务的功能模块称为虚拟网关，虚拟网关是远程用户访问 VPC 内网资源的统一入口。远程用户在 Web 浏览器中输入虚拟网关的 IP 地址，并在虚拟网关登录界面输入用户名和密码，虚拟网关将会对用户进行身份认证。身份认证通过后，虚拟网关会向远程用户提供可访问的内网资源列表，远程用户点击资源列表链接即可访问对应资源。

- 用户登录：远程用户通过Web浏览器（客户端）登录虚拟网关，请求建立SSL连接。虚拟网关向远程用户发送自己的本地证书，远程用户对虚拟网关的本地证书进行身份认证。认证通过后，远程用户与虚拟网关成功建立SSL连接。
- 用户认证：虚拟网关对远程用户进行用户认证，验证用户身份。用户认证可以选择以下四种方式之一：本地认证、服务器认证、证书匿名认证、证书挑战认证。
- 角色授权：用户认证完成后，虚拟网关查询该用户的资源访问权限。用户的权限分配通过角色实现，先将具有相同权限的用户/组加入某个角色，然后角色关联可访问的业务资源，角色是联系用户和资源的纽带。
- 资源访问：虚拟网关根据远程用户的角色信息，向用户推送可访问的资源链接，远程用户点击对应的资源链接进行资源访问。

3.2.3.4.12 DNS 云解析服务

云解析服务(Domain Name Service，DNS)提供高可靠、高扩展的 DNS 服务，

把人们常用的域名(如 www.example.com)转换成用于计算机连接的 IP 地址(如 192.1.2.3)。云解析服务可以让您直接在浏览器中输入域名，访问网站或 Web 应用程序。

提供 VPC 内生效的内网域名与私网 IP 相关联，为云上资源提供 VPC 内的域名解析服务。内网域名可以随意创建，不需要购买和备案。

3.2.3.5 **操作系统建设方案**

3.2.3.5.1 linux 操作系统

红帽企业 Linux 6 是一个长期开发的、可预测的操作平台的第六代。通过灵活 地作为虚拟主机、虚拟客户机或者在云环境中物理硬件上部署，红帽企业 Linux 为下一代数据中心提供了理想的基础。它保证了长期的稳定性，同时继续创新 并提供增强特性 - 实现了创新与稳定性的最佳结合。

通过与业内主要厂商结成合作伙伴关系，红帽能够保证该平台在大量系统和应 用中的稳定性。借助嵌入式工程设计和深层协作，红帽在该技术的商业部署领 域处于领先地位。客户通过及时的服务包和中期版本的发布而获益。

红帽企业 Linux 的模块化架构允许在增强功能时不会影响应用接口。应用在更新时不需要重新构建或重新认证，因为应用编程和二进制接口 (API/ABI) 在所有红帽企业 Linux 版本中保持不变，无论是物理、虚拟还是云部署模式。这意味着红帽数千个认证应用组成的巨大生态系统随时保持可用，避免了供应商每次升级软件时需要昂贵且耗时的重新测试而带来的延误。

其它特性保证了红帽企业 Linux 的稳定性和可信性。软件 RAID、存储多路径支 持和网络接合在网络和存储区域提供了弹性。文件系统能力(例如屏障和 TRIM 支持)保证可数据安全，并提供了瘦配置能力，而逻辑卷管理提供了磁盘提取功能。这些新特性不断发展，使红帽企业 Linux 成为最稳定、最可信的 IT 平台之一。

- **灵活性**

红帽企业 Linux 为客户根据其独特环境定制操作系统而提供了全面的选项。红帽企业 Linux 6 包括了新定义的特色组件群，允许轻松地选择不同的特性，涵盖了从针对基础运行时环境的最小安装，到全套供选择的特性，包括存储选项、系统管理、图形化界面和管理实用工具。除了支持大量的基础设施选项外，红帽

企业 Linux 6 还包括完整的一套开源应用。借助所支持的应用，包括从 Web 基础设施到数据库与开发框架，红帽企业 Linux 6 的安装可满足大量工作负荷的需求。

除了可灵活选择的特性外，红帽企业 Linux 还支持包括行业标准服务器和主机 的大量硬件，以及用于通过扩展更新支持 (EUS) 和扩展生命周期支持 (ELS) 而 延长硬件生命周期的新订阅选项从而提供了灵活部署能力。

客户还可以通过自动化部署特性 可实现运作灵活性，例如红帽网络的快速启动 工具、自动系统更新和审计能力。红帽网络及红帽网络卫星的离线版本有助于 企业降低每个系统的部署和管理成本，通过自动和集中完成例行任务而缩短停 机时间，并创建一致的环境。

- **集成的虚拟化**

红帽的虚拟化技术易于采用，因为它是红帽企业 Linux 平台不可分割的一部分。借 助基于内核的虚拟机 (KVM) 技术，红帽的虚拟化能力已经集成到红帽企业 Linux 中，并能够利用 Intel® 和 AMD® 处理器平台提供的最新硬件虚拟化能力。红帽企 业 Linux 的模块化设计允许客户选择在何时以及何处使用虚拟化。如果需要更大 的灵活性，客户能够部署红帽企业 Linux 和 Microsoft® Windows® 作为红帽企业 Linux 虚拟化环境中全面支持的虚拟机。红帽企业 Linux 还支持多种虚拟化应用案 例，包括现有软件堆栈的硬件抽离、数据中心整合以及虚拟化集群和私有云。

除了核心虚拟化外，红帽企业 Linux 通过 SR-IOV 和 nPIV 标准对高级虚拟化 I/O 能力提供了领先的支持。由红帽公司开发并且被其它操作系统采用的标准虚 拟化管理基础设施 libvirt，为定义、管理和监控虚拟机提供了灵活的接口。

- **扩展性与性能**

  红帽企业 Linux 6 的设计提供了高性能和扩展性，而不会损害数据完整性。它可 以扩展至 4,096 个 CPU 和 64TB 的 RAM，为支持未来几代的硬件奠定坚实的 基础。在这个广泛框架内，红帽企业 Linux 6 提供了对多种网络基础设施的支持， 例如 Infiniband 和以太网，并支持存储基础设施，例如 FCoE 和 iSCSI，同时支 持传统 nAS、San 和

DAS 设备。

红帽企业 Linux 还提供了卓越的性能，并可从桌面扩展到工作站，从刀片扩展 到机架环境，从单 CPU 系统扩展到最大型的 SMP 服务器和大型机。随着硬件 升级持续提供更多的处理和存储能力，红帽企业 Linux 允许客户选择横向扩展 和纵向扩展战略与平台架构而满足其业务要求，从而充分利用这些进步。

- **扩展性与性能**

红帽与合作伙伴持续地开展合作，向客户提供先进的功能。例如，虚拟化性能 的改进使得在红帽企业 Linux 平台上部署任何应用工作负荷成为现实，即使是 I/O 受限的应用。最近的虚拟机性能的重大改善是通过 I/O 优化而实现的，包括 对新硬件能力的支持，例如 10GB 的 SR-IOV 适配器和 nPIV。这将使 I/O 受限 的环境的开销降低到 5% 以下，为部署全新的应用提供了机会，如数据库、交 易处理和文件服务器。

红帽正与硬件合作伙伴联手，将最近推出的高可靠性、可用性、可维护性 (RAS) 以及扩展能力融合到主流架构中，从而最大限度缩短停机时间，提高可用性， 并保护数据安全。

基于红帽企业 Linux 的系统在各类行业标准基准测试中取得了领先的成绩，例 如测量 Web 服务的 SpecWeb；针对大型数据仓库的 TPC-H；以及针对服务器整合的 SpecVirt。在多种工作负荷上和不同 IT 架构中，红帽企业 Linux 6 为从 新服务器硬件中获得最大收益提供了基础。

- **安全性**

红帽企业 Linux 的安全性首先从核心特性开始，即安全增强型 Linux (SELinux)。 SELinux 由红帽和美国国家安全局 (NSA) 共同开发，为执行基于角色的接入控 制和多级安全提供了强大且灵活的 MAC 框架。对 SELinux 的支持已经融合到 平台的各个部分，包括虚拟化，无论是哪种虚拟机操作系统，都可以提供关键 的虚拟机隔离能力。凭借全面的应用策略和对系统权限的全面审查，红帽企业 Linux 6 使得 SELinux 的使用比以往任何时候都容易。

除 SELinux 之外，红帽企业 Linux 还包括系统防火墙、审计能力和系统封装与 文件完整性验证工具，组成了一个涵盖多种部署模式的完整安全架构，包

括从 面向互联网的服务器到可信的计算机。核心技术的背后是红帽安全响应团队， 该团队在消除安全漏洞方面是公认的行业领导者。红帽企业 Linux 为客户及其 应用提供了无与匹敌的安全环境。

- **跨物理、虚拟和云环境的敏捷性**

红帽企业 Linux 6 允许企业在数据中心内部署物理、虚拟和云计算环境。凭借 直接集成到内核中的 KVM，红帽企业 Linux 6 技术可适应所有环境的要求，从 而降低复杂性，提高效率，并最大限度减少管理开销，同时充分利用操作平 台的技能。集成的虚拟化可实现互操作式的物理和虚拟部署，而精细的计算资 源 (CPU、内存、网络和 I/O) 控制允许企业管理应用或虚拟机的服务等级协议 (SLA)。此外，电源管理增强功能减少了系统的碳排放量。

3.2.3.5.2 Windows 操作系统

Windows Server 2022 内置混合云功能让本地服务器可以像云原生资源一样在 Azure 云平台进行统一的管理，高级多层安全性硬件、软件、数据、传输一层层加固，不给病毒和恶意攻击可乘之机。

Windows Server 2022 自动提供用户需要的服务包括监控、备份、补丁、安全等还有“体检报告”，主动检测自动修正。

微软公司在 Windows Server 2022 中引入了许多提升安全性的功能。IT 和 SecOps 团队可以利用 Secured-core server 高级保护功能和预防性防御功能，跨硬件、跨固件、跨虚拟化层，加强系统安全性。新版本增加了较为快速、安全性较高的加密超文本传输协议安全（HTTPS）和行业标准 AES-256 加密，支持服务器消息块（SMB）协议。

Windows Server 2022 可以通过与 Azure Arc 连接，在本地 Windows Server 2022 获取云服务。此外，在 Windows Server 2022 中，用户可以利用 File Server 增强功能，例如 SMB Compression，通过在网络传输时压缩数据来改善应用程序文件传输。Windows Admin Center 可帮助用户体验现代的服务器管理，例如在连接 Azure 的场景中提供新的事件查看器和网关代理支持。

在 Windows Server 2022 中，用户还可以看到一些 Windows 容器的改进。Windows Server 2022 提高了 Windows 容器的应用兼容性，其中包括用于节点配

公共资源交易平台投标专用

置的 HostProcess 容器。它支持 IPv6 和双协议栈，还支持使用 Calico 实施一致的网络策略。

支持 WSL2，微软开始随 Windows 一起发布完整的 Linux 内核，从而实现完整的系统调用兼容性。此外，Linux 发行版的性能明显优于基于 WSL 原始版本的发行版。Linux 现在运行在一种虚拟机 (VM) 中，但它被设计成比传统 VM 更轻量级和原生体验。

3.2.3.5.3 国产化操作系统

统信服务器操作系统 V20 提供多种高可用集群解决方案和多种高可用机制，为资源转移、数据备份、失效节点恢复等服务予以有效支撑，最大限度减少业务系统服务中断时间，将因软件硬件等故障造成的影响降至最低。同时提升了服务最大可用性和资源最大利用率，保障用户业务系统可对外不间断提供服务。

统信基于多年对 Linux 操作系统产品的研发经验，在设计研发统信服务器操作系统 V20 时，采用了稳定版 Linux 内核，结合服务器产品的功能需求和特性，对内核、编译器、系统软件进行合理的定制和优化，对文件系统进行开发和维护，对操作系统的基础库、服务运维环境、服务应用以及开发环境进行深度完善，在保障系统稳定和安全等运行的同时，也注重提高系统的整体性能，配合系统所提供的多种企业级高可用集群解决方案及机制，充分提升操作系统的稳定性。除此以外，统信服务器操作系统 V20 采用内核热补丁升级及漏洞修复机制。用户在升级最新的系统补丁，修复内核缺陷和安全漏洞时，无需重启系统或中断业务应用，最大程度上减少系统关机和业务中断时间，增加系统可靠性。统信服务器操作系统 V20 发布前，通过在大规模全 CPU 架构整机上采用 LTP 工具测试，在 LTP Stress 7×24 小时长时间高负荷条件下的压力测试无宕机，测试用例通过率超过 98%，且经上述场景下予以卸荷后，在。不超过 60 秒内实现系统以及各应用流畅运行。另外，在一些关键行业、特定场景，可根据用户需求的不同，为其提供内核定制、系统服务裁剪与扩充、性能调优、应用迁移指南等服务。

统信服务器操作系统 V20 在充分保障安全性、稳定性的同时，极度重视系统性能的调校，通过引进国内外知名且成熟的技术与工具，从对系统在人工智能、统信服务器操作系统 V20 白皮书 统信软件技术有限公司 ©版权所有 第 11 页大数据、云计算、Web 服务、容器等各应用场景中各项性能数据分析的基础上，

基于“破除瓶颈桎梏、资源利用充分”原则，对系统性能给予最大化调优。

统信服务器操作系统 V20 从安装部署、初始化设置、异常自动化处理、运行负载监控、运行负载均衡调度、定时备份等方面出发，基于多款开源运维工具进行功能扩展，向服务器运维管理人员提供可视化运维支持，节省管理员在各环节的维护时间，提升运维效率。

3.2.3.5.3.1 统信服务器操作系统

统信服务器操作系统 V20 汲取国内外主流社区技术栈优势，深入技术底层结合国内外设计标准与规范（具体规范和标准详见：“3.5 设计标准”）以及各类用户业务应用需求，积极开展技术创新，全面支持国内外主流 CPU 架构（AMD64/ARM64/ MIPS64/SW64/LoongArch 等）和处理器厂商，在各种应用环境中，满足强安全、高可用、高性能、易维护以及高可靠等要求，是一款构建信息化设施环境的基础软件产品。统信服务器操作系统 V20 采用多模态（用户态、系统态等）、模块化的设计理念，全面支持在物理、云（公有云、私有云以及混合云）或超融合环境上构建生产环境，并通过连接传统和新基础设施（如软件定义网络 SDN、软件定义存储 SDS 等）简化用户 IT 环境，帮助用户环境切换，为软件定义 IT 时代转型铺平道路，为加速信息技术创新奠定坚实基础。

统信服务器操作系统 V20 通过了工信部对电子政务信息化指南要求中针对通用型操作系统的标准化测评以及公安部对信息安全技术操作系统安全技术要求四级评测，基于强化服务器操作系统网络服务、数据服务、文件服务、进程管

理等核心技术服务，建立了全国产化生态支持体系并提供全栈服务器操作系统丰富生态，从而确保了政务数字化、企业数字化等数字化转型有序推进，在国产化“新基建”中提供灵活性和多样性选择，并使得在各业务应用场景中的网络化、信息化、数字化、智能化等一体化建设得以顺利推动。

整个操作系统包括系统层和应用层。系统层中 Linux 内核向下控制硬件层资源，并管理操作系统资源对象：包括进程管理、内存管理、文件系统、设备驱动以及网络，向上则向应用层提供系统调用接口。应用层：用户可按人工智能、大数据、虚拟化、容器、云计算等应用场景选择应用组件和工具。

统信高度重视系统以及各类数据的安全性，统信服务器操作系统 V20 在充分

继承 Linux 安全特性的基础上，根据 SDL 规范和自身产品的特点，结合等保2.0 和可信计算等要求，构建了系统内核、系统应用、主动防御以及安全合作等全方位的企业级系统安全防护体系。统信服务器操作系统 V20 围绕全栈国密、身份鉴别、访问控制、安全审计、数据保护、网络安全保护等，在运行安全、资源利用、可信度量、安全策略等维度，全方位加强防御纵深，采用 TCM/TPM/TPCM 可信启动、统一 PAM（Pluggable Authentication Modules，可插拔验证模块）认证模块、多因子认证，以及国密算法和 CVE 漏洞发现与修复等多种安全策略和安全机制，予以有机组合，使系统及数据的安全性得以持续增强并加固，有效抵御来自系统外部的入侵，将威胁降至最低。

3.2.3.5.3.2 银河麒麟服务器操作系统

银河麒麟服务器操作系统是麒麟软件有限公司发行的简单易用、稳定高效、安全可靠的新一代操作系统产品；同源优化支持六大自主 CPU 平台；提供经典和创新风格的用户体验，操作简便，快速上手；针对国产平台深入优化大幅提升系统的稳定性和性能；应用商店提供精选数百款常用软件，包括麒麟系列自研应用、工具软件和第三方商业软件，同时兼容安卓原生应用，极大丰富 Linux 生态；提供多 CPU 平台统一的在线软件升级仓库，支持版本在线更新，让您的产品与时俱进。

产品特点：

同源优化支持自主 CPU：同源构建支持六大国产平台，内核、核心库和桌面环境等所有组件基于同一套源代码建，并面向各自主 CPU 及服务器整机进行了针对性优化适配，为不同平台的软硬件生态提供兼容一致的开发和运行接口，为管理员提供一致的运维管理体验。

本质安全：基于自主软硬件、密码技术的内核与应用一体化的内生本质安全体系：自研内核安全执行控制机制 KYSEC、生物识别管理框架和安全管理工具，支持多策略融合的强制访问控制机制；支持国密算法 SMx 和可信计算 TCM/TPCM、TPM2.0 等；达到 GB/T 20272 第四级、B+级安全技术要求。

虚拟化及云原生支持：优化支持 KVM、Docker、LXC 虚拟化，以及 Ceph、GlusterFS、OpenStack、k8s 等原生技术生态，实现对容器、虚拟化、云平台、

大数据等云原生应用的良好支持。

高可靠性：通过 XFS 文件系统、备份恢复、网卡绑定、硬件冗余等技术和配套磁盘心跳级高可靠集群软件，实现主机系统和业务应用的高可靠保护。

国产平台深入优化：针对不同自主 CPU 平台在内核安全、RAS 特性、IO 性能、虚拟化和国产硬件（桥片、网卡、显卡、AI 卡、加速卡等）及驱动支持等方面优化增强，以及工控机支持。

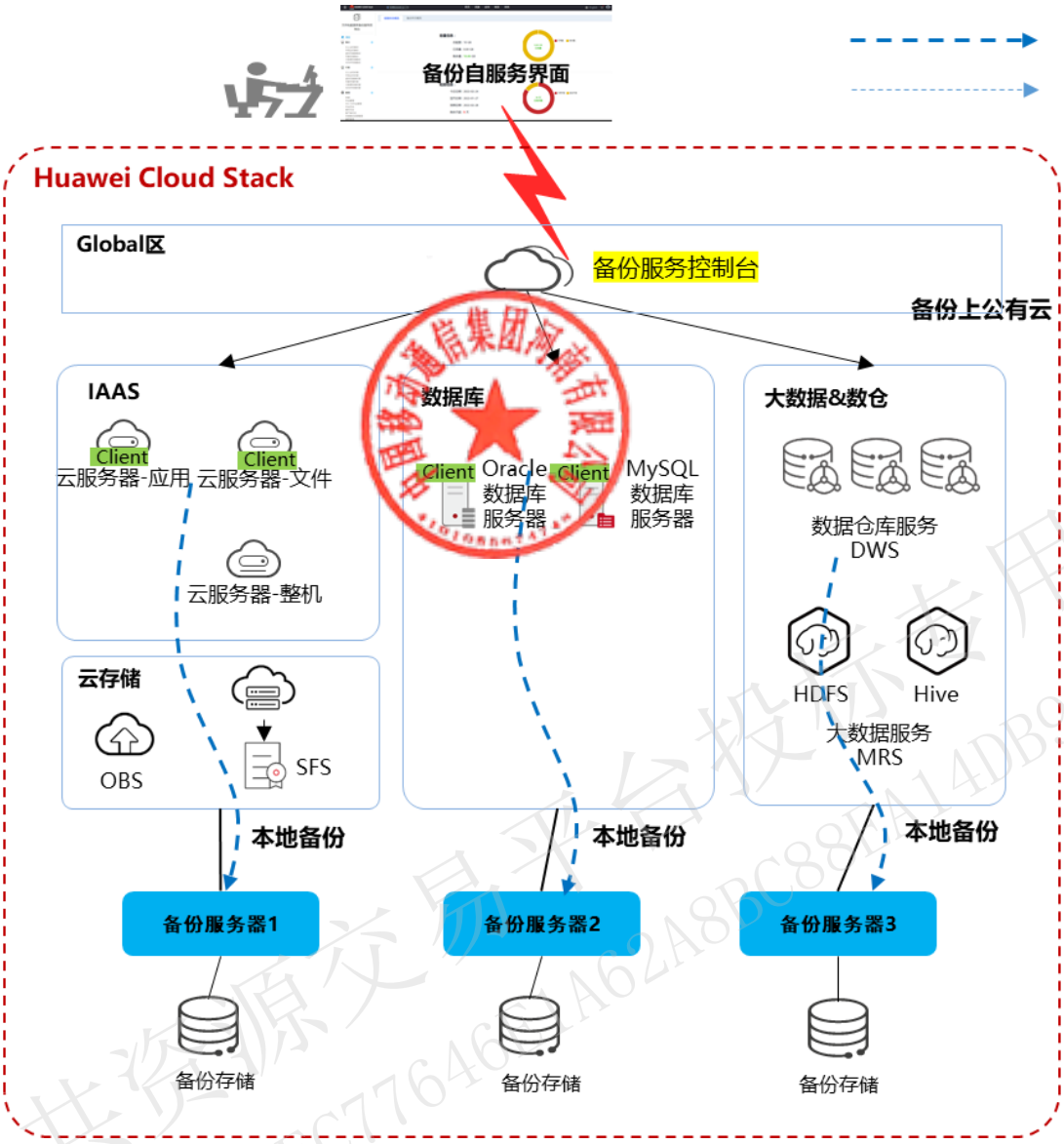
可管理性：提供图形化管理工具和统一的综合管理平台（SystemCenter），实现对物理服务器集群运行状态的监控及预警、对虚拟化集群的配置及管控、对高可靠集群的策略定制和资源调配等功能。

3.2.3.6 备份建设方案

3.2.3.6.1 整体架构

如下图所示为本项目的备份方案架构。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9



本项目采用 HCS 统一备份服务 HBR 作为云平台的备份软件，云上的虚拟机，数据库，大数据等提供统一的备份服务能力。

- 与MO统一界面、统一管理：构建备份服务化管理平台，统一方案，统一运营管理，节省运维费用；
- 从应用到存储数据的全面保护、统一管理：一套方案全栈保护云上业务，实现云主机，数据库，对象/文件存储，大数据的统一备份；
- 数据库任意时间点保护：数据实现保留短周期内任意IO操作，实现短周期内任意历史时间点数据恢复；

备份原理如下：

通过 ManageOne 接口和华为存储接口实现了 HCS 云主机整机的 ServerLess 备份恢复功能。

公共资源交易平台投标专用

数据库备份：支持传统数据库、国产数据库备份，调用数据库备份接口或工具，获取数据并备份。

对象存储备份：使用 S3 接口从对象存储下载和上传数据，数据通过多线程备份保存到备份介质中。

大数据备份：通过调用大数据备份接口或者工具，获取平台数据并备份。

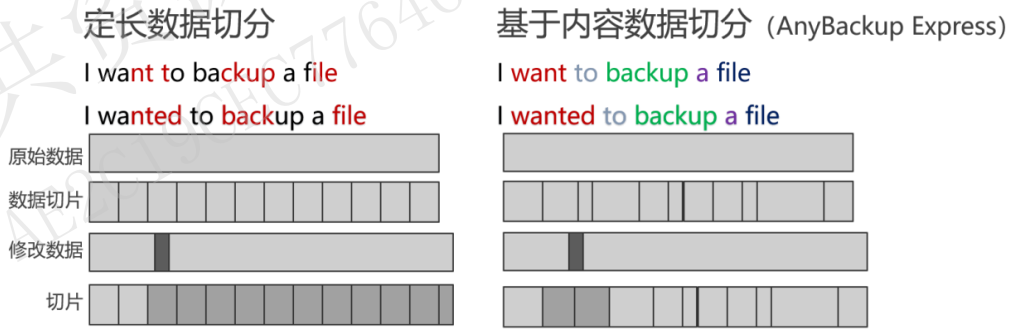
虚拟化备份：通过快照及 CBT 技术实现虚拟机备份。

备份支持重删技术

1. 基于内容的变长数据切分

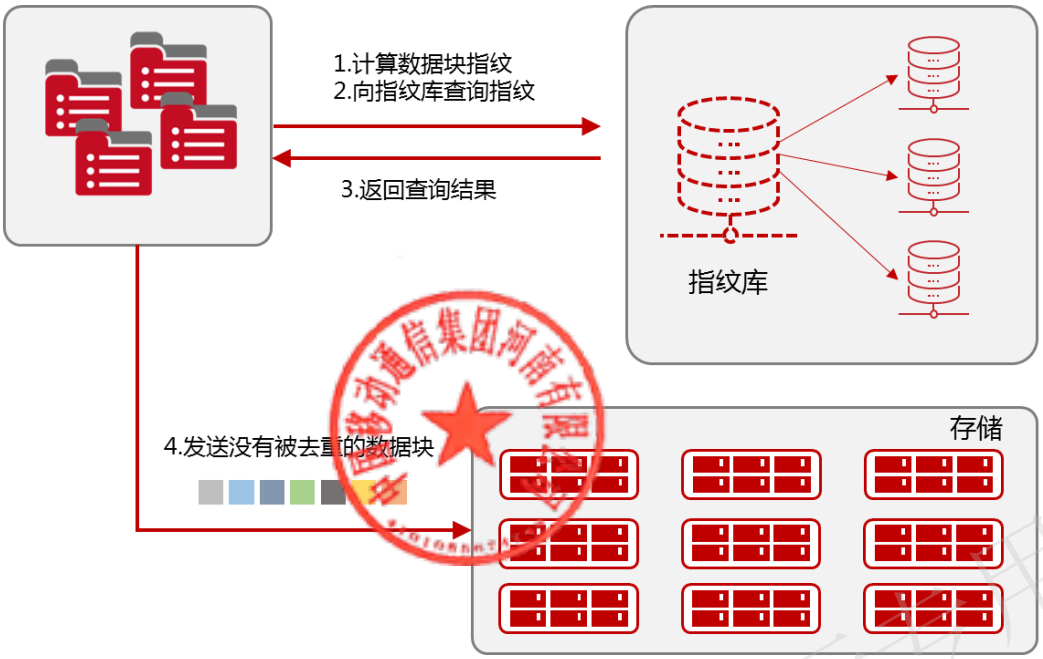
第四代重复数据删除技术使用基于内容的变长数据切分算法。该算法可以智能识别已修改的数据和未修改的数据，从而避免因修改数据位移而导致的未修改数据切分到新数据块中的问题，最大限度地提升重删性能和重删率，目的在于不备份任意一个冗余数据。

与定长切片算法相比，基于内容的变长切片方式能够达到更高的数据去重比率。而定长切片按照固定大小切分文件或数据源，如果一个文件在文件开始新增或减少一个字符，将导致所有切片的指纹发生变化，最差的结果是备份两个仅差一个字符的文件，导致重删率为 0。



2. 源端重复数据删除

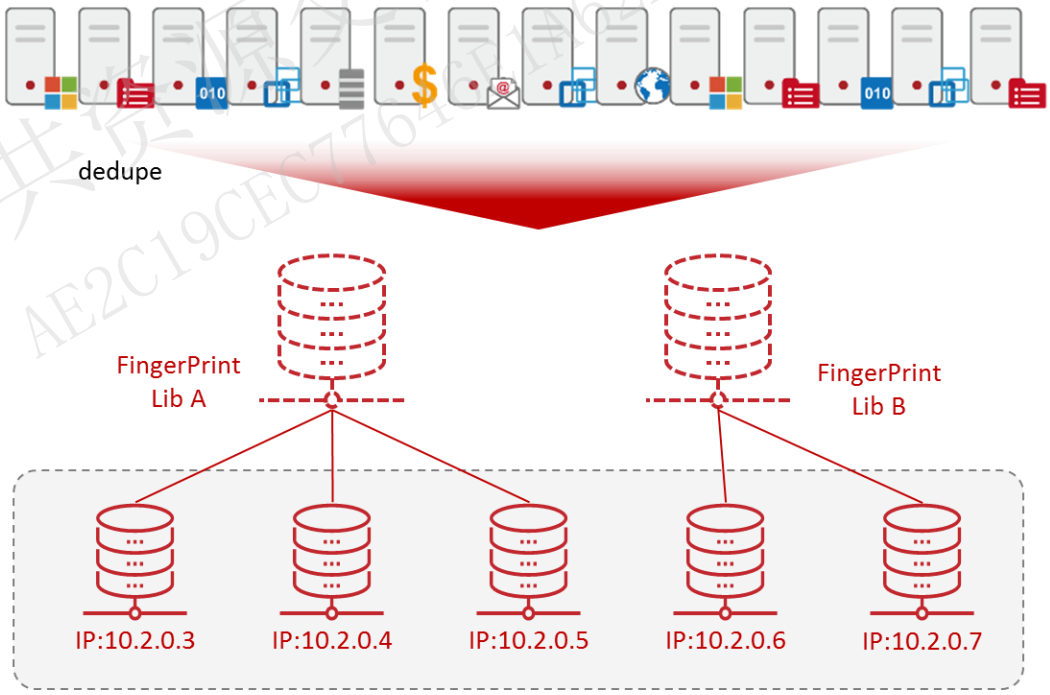
将数据或文件使用智能的基于内容的可变长数据切分算法进行切片后，数据块通过哈希算法进行唯一标记，即指纹（Fingerprint），并在指纹库中寻找相同的指纹。如果存在相同指纹，则表示已保存了相同的数据块，介质服务器则不再保存此数据块，而是引用已存在的数据块，从而节省更多的备份空间，同时有效的节约传输时所需的大量带宽，实现数据传输和存储的最大精简。



3. 并行重删

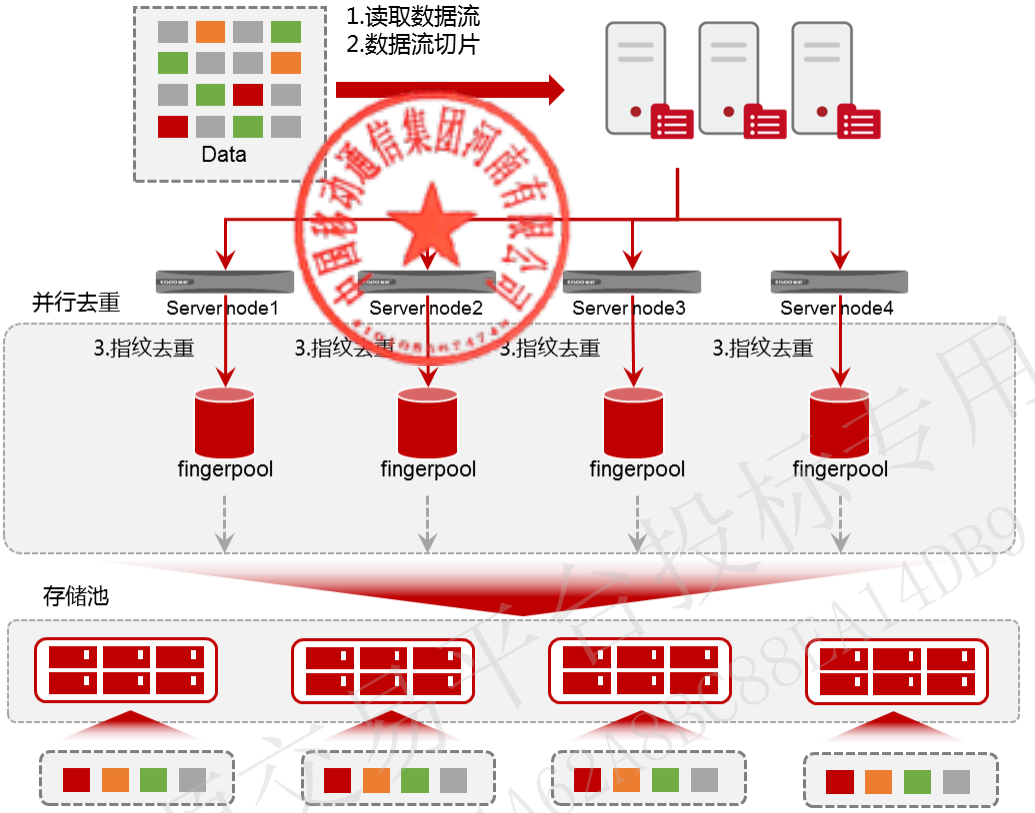
传统重删模式大多基于单个节点进行，此方案在大数据时代，容易面临数据访问、处理性能不足，存储空间资源紧张等挑战。

备份系统采用并行重删技术，通过在多个不同的节点上构建指纹库，并将指纹并行分布于多个节点，有效解决单点性能和存储空间压力问题。



传统重删方式采用磁盘读写指纹方式，会产生大量的随机 IO，严重影响性能。而并行重删技术采用内存级指纹库进行重删，所有指纹读写全部保存于内存中，

从而提升指纹查询和处理效率，并且减少了因磁盘中指纹库增大所导致的随机IO压力。当指纹库不再需要进行备份时，将指纹同步到磁盘当中。指纹库构建在不同重删节点上，而生产数据可以基于多个不同的指纹库，执行并行重删。



并行重删工作流程

通过指纹库策略，可以将重复利用的数据按顺序、连续地保存在同一个空间内。如此，即可实现：一，可以减少全局重删时每次都要查找全部指纹的时间损耗；二，可以最大限度利用存储的读缓存机制，尽量减少因随机读磁盘引起的频繁磁盘寻道的切换，提升恢复效率；三，可以做数据清理。

备份支持增量备份技术

传统的备份方案大多采用周期性的“完全备份+增量备份”策略，其增量备份大多不可持续的，经过一段时间就必须执行一次完全备份。因而传统的备份方案经常面临备份窗口过大的问题，而且其增量备份数据的恢复效率相对低下，因为每个时间点的恢复都依赖于上一次完备副本和上一次完备副本后的所有增量副本，恢复操作需要进行逐个迭代恢复。此外，过期增量数据的清理操作也受限于备份副本之间的依赖关系，不一定能及时被清除。

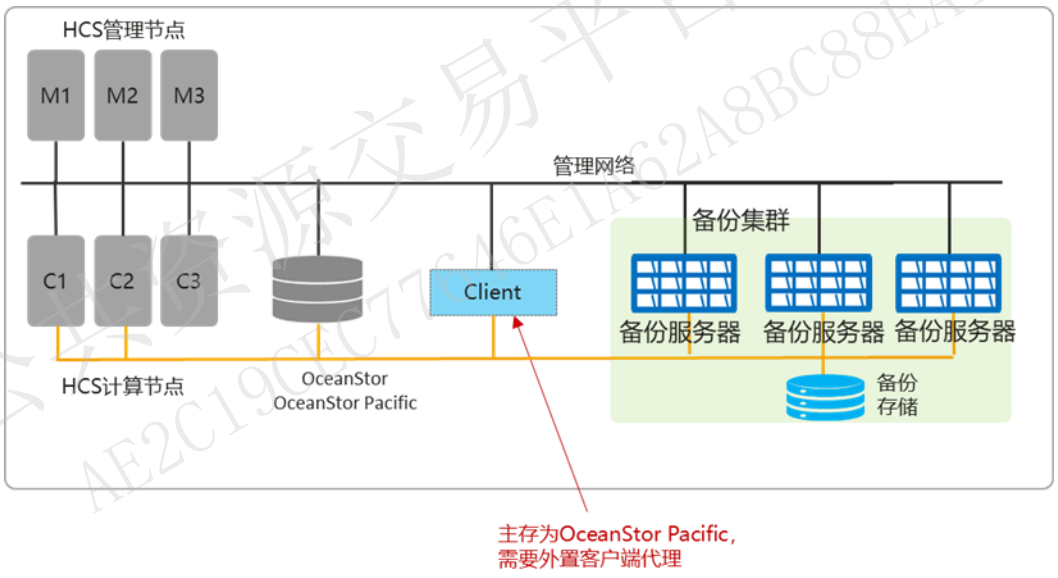
备份系统采用永久增量备份技术，初次备份对所有数据进行完全备份，之后只对新增加或改动过的数据做增量备份。此方案的增量备份数据是持续的，而且每个增量备份的数据副本将自动合成为完全副本，方便恢复。因而永久增量备份能够大幅度减少备份时间，节省备份数据所需的存储空间，且提升了恢复效率。

永久增量备份适用于单个应用数据量大，执行一次完全备份比较费时费力的应用场景。若用户备份数据量小，也可使用周期性的完备和增备方案。

永久增量备份工作原理如下：

1. 首次备份所有数据，且为每个数据块建立索引连接。
2. 第二次及以后的备份，只对新增的数据进行备份。
3. 将增量数据索引与上一个副本的索引进行合成，生成新的完整副本。
4. 恢复时，指定时间点，即可直接恢复合成的完整副本。

3.2.3.6.2 云主机备份



备份流程：

①对云主机的云硬盘创建一致性快照；

②通过存储快照差异比对获取有效数据块或增量数据块；

③读取变化数据块，备份至备份系统；

④删除上一次备份保留的快照。

恢复流程：

①用户选择要覆盖的云主机，云硬盘大小和数量需要与原云主机保持完全一致；

公共资源交易平台投标专用
AE2C19CEC776E16E1A62A8BC88EA14DB9

②将要覆盖的云主机对应的云硬盘挂载到 Client 所在服务器；

③Client 从介质中读取备份数据，写入步骤 2 中挂载过来的卷中。直至云主机的所有云硬盘数据恢复完成；

④恢复完成后，卸载卷。云主机覆盖恢复完成。

3.2.3.6.3 操作系统/文件备份



文件系统备份流程图

在需要保护的 PC 或服务器上安装备份客户端软件，并连接管理控制台。备份客户端软件会识别客户端计算机的文件系统，并通过备份 API 读取客户端计算机上的文件数据，将数据向备份介质服务器备份。备份管理控制台是整个备份系统的纽带，负责向客户端软件和介质服务器发送控制信息，管理整个备份任务的运行。

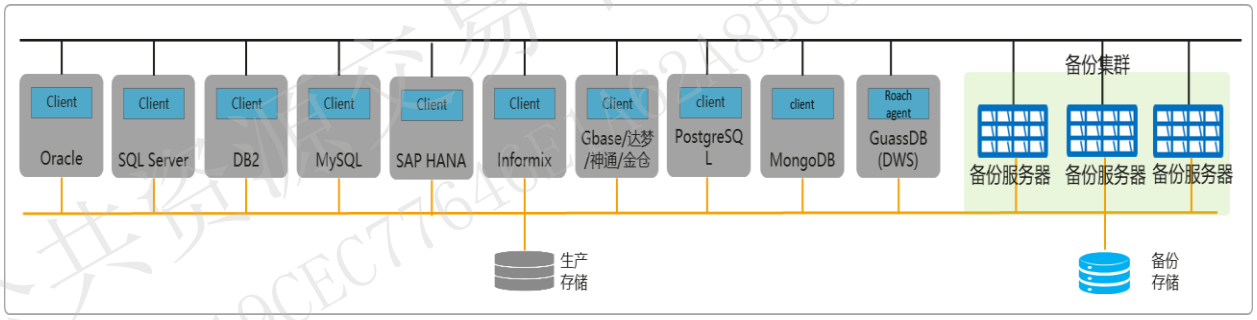
NAS 需要先挂载到某个主机下，备份流程与本地文件系统备份流程一致。统一备份文件系统备份模块支持备份非结构化的文件系统，其功能特点如下：

- 支持的备份类型包括：完全备份、增量备份和永久增量备份。
- 恢复粒度：支持细粒度恢复，最小粒度为恢复单个文件。支持跨文件系统恢复，例如恢复到EXT3、EXT4、NTFS等文件系统。
- 备份策略：支持设计备份策略，用户可以根据需要选择定时备份任务的执行策略。
- 永久增量备份：支持永久增量备份，提升备份效率，节省存储空间。
- 重复数据删除：支持块级重删，减少备份数据的传输量，缩短备份窗

口，节省备份数据传输所消耗的网络资源以及存储空间。

- 安全的数据保障：统一备份采用了AES256和SM4高级加密标准算法，支持开启传输和存储加密。
- 数据保留策略：支持两种数据保留策略，数据保留期限或保留副本数，开启后可对备份存储空间循环利用。
- 灵活的恢复方案：文件系统恢复支持原机原位置恢复，或原机指定位置恢复，以及异机恢复。
- 增量备份以单个文件为备份粒度，通过比较最近的修改时间和备份时间判定该文件是否需要备份，并以此为基础进行增量备份。
- 自定义脚本：支持添加自定义脚本，在任务执行前、执行成功后、执行失败后触发。由于自定义脚本可完全由用户自行编写，所以可以完全适应各类场景。

3.2.3.6.4 数据库备份



数据库备份采用两种方案，针对不同的数据库采用不同的备份方式。

方案 1：调用数据库接口直接备份恢复：

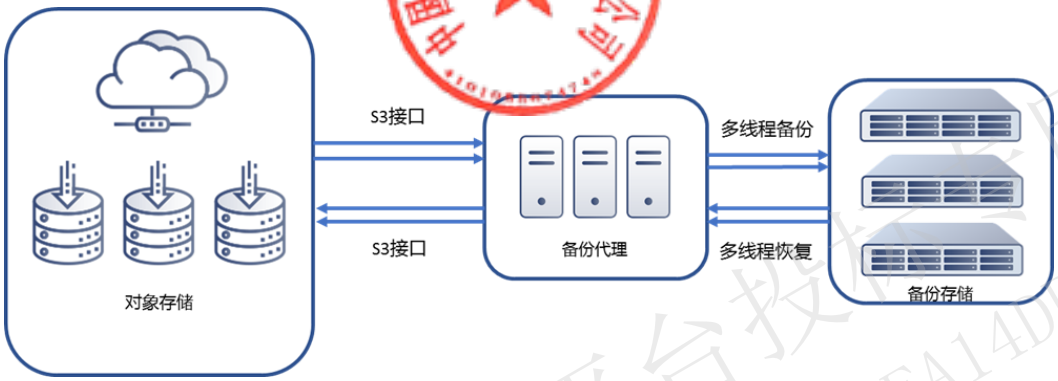
- Oracle：RMAN（Recovery Manager）
- SQL Server：VDI（Virtual Device Interface）
- DB2：Vendor
- MySQL：MySQL Plugin
- SAP HANA：hdbsql

方案 2：调用数据库工具先将数据导出到临时存储空间，再备份临时存储空间文件：

公共资源交易平台投标专用

- Informix：Ontape
- GBase：Gbase API
- 达梦：backup
- 金仓/神通：export，import
- MongoDB：mongodump，mongorestore
- GuassDB（DWS）：Roach

3.2.3.6.5 对象存储备份



对象存储备份原理：对象存储备份、恢复功能在客户端上使用 S3 接口从对象存储下载和上传数据，数据通过多线程备份保存到备份介质中以及从备份介质中取出。

完全备份：将选定的对象存储数据源备份到指定备份服务器中，每次执行时直接将所有的数据备份到备份介质中，并产生一个时间点，用于记录备份内容；

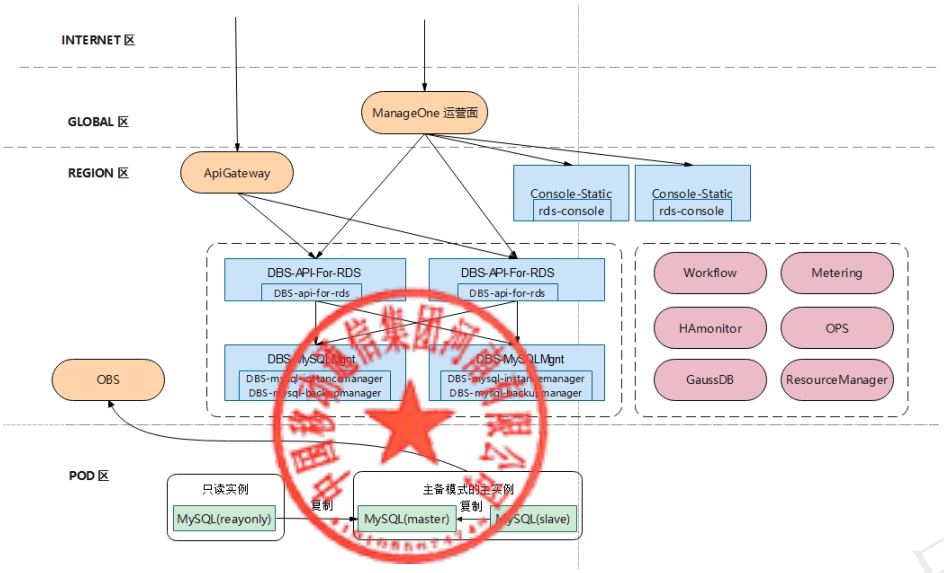
增量备份：是基于上一次备份（可以是完全也可以是增量），将新增的数据备份到备份介质中，同时产生相应的时间点。利用对象存储桶日志快速识别变化文件，提高增量备份效率，降低 PRO，并且减少对生产系统的影响。

3.2.3.7 数据库建设方案

3.2.3.7.1 MYSQL 数据库服务

（一）系统架构

云数据库 RDS（Relational Database Service，简称 RDS）是一种基于云计算平台的稳定可靠、弹性伸缩、便捷管理的在线云数据库服务。



MYSQL系统架构

节点类型	说明	部署原则
Console-Static	用于部署所有服务的静态资源，包括RDS for MySQL。	使用2台虚拟机，采用集群部署方式。
DBS-API-For-RDS	RDS服务的API节点，部署DBS-api-for-rds服务	使用2台虚拟机，采用集群部署方式。
DBS-MySQLMgnt	RDS for MySQL实例管理节点，部署DBS-mysql-instancemanager和DBS-mysql-backupmanager两个服务	使用2台虚拟机，采用集群部署方式。

表 0-3 MYSQL组件列表

（二）服务能力

云数据库 RDS 服务具有完善的性能监控体系和多重安全防护措施，并提供了专业的数据库管理平台， 让用户能够在云上轻松的进行设置和扩展云数据库。通过云数据库 RDS 服务的管理控制台，用户无需编程就可以执行所有必需任务，简化运营流程，减少日常运维工作量，从而专注于开发应用和业务发展。

公共资源交易平台提供专用

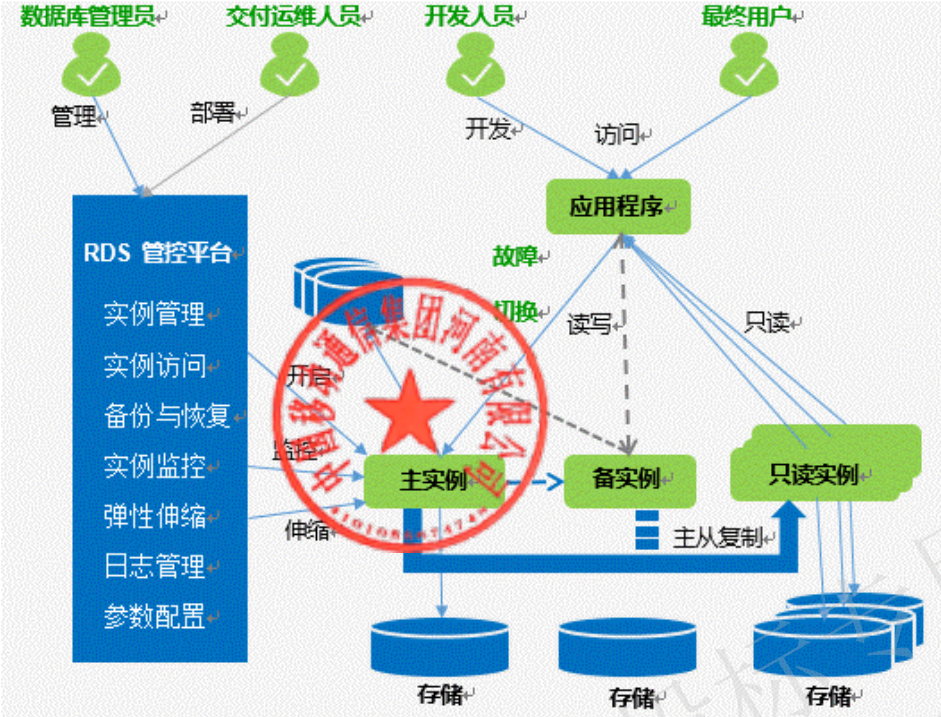


图 0-2 MYSQL功能架构

- 数据库类型及版本：MySQL 5.6、5.7
- 数据安全：多种安全策略保护数据库和用户隐私，例如：VPC、子网、安全组、VPN、SSL等，支持数据存储卷加密。
- 数据高可靠：数据库数据可靠性高，在99.9999999% （ 9个9）以上；备份数据可靠性高达99.999999999% （ 11个9）
- 实例访问：多种访问方式，包括：内网IP访问、公网 IP 访问、VPN 访问
- 实例管理：支持实例的增、删、改、查、重启等生命周期管理
- 实例监控：支持监控数据库实例 OS 及 DB 引擎的关键性能指标，包括计算/内存/存储容量使用率、I/O活动、数据库连接数、QPS/TPS、缓冲池、读/写活动等
- 弹性伸缩：水平伸缩：增删只读实例（最多5个）；垂直伸缩：实例规格变更，存储空间扩容（最大10 TB）
- 备份与恢复：备份：自动备份、手动备份，全量备份、增量备份，备份文件的增、删、查、复制等生命周期管理。恢复：恢复到备份保留期内任意时间点（Point-In-Time Recovery, PITR）/某个全量备份时间

公共资源交易平台技术专用
AE2C19CE0776461A6248DC88EA14DB9

点，恢复到新实例/原实例。备份保存周期高达732天

- 日志管理：支持查看慢 SQL 日志、错误日志、下载等
- 参数配置：数据库管理员可以根据监控和日志等信息，对数据库引擎参数进行自定义设置，从而优化数据库。参数组的增、删、改、查、重置、比较、复制等生命周期管理，方便用户批量管理实例的数据库引擎参数

3.2.3.7.2 Oracle 数据库服务

- **概要**

过去 30 年来。信息技术成熟到全球经济几乎全都仰赖电子撷取、分析与分享信息的地步。

各企业持续扩大自己的信息基础架构,想要满足以更短时间存取信息而且不断成长的业务需求。然而,企图勉强结合青黄不接的技术与流程,导致各企业信息技术(IT)基础架构 普遍的严重复杂性与效率不彰。由于日常作业完全仰赖信息技术基础架构,这种复杂性威胁到了企业快速应变的能力。

Oracle Database 11g 是供绝佳创新,使各企业能够更快速应变。高成本的负担与瞬息万变的业务需求息息相关,各企业可以仰赖 Oracle Database 11G 帮助创新,以妥善掌控、具备成本效益的方式执行 IT 变革。

Oracle Database 11g 解决阻碍各 IT 组织进步的核心问题:自信满怀地执行变革的能力。运用 Oracle Database 11g,各企业可以统合所有信息,而简化自己的信息基层架构。

Oracle Database 11q 不断地为更高价值的规划工作而释出宝贵的技术资源,使管理工作自动化进而建置崭新的业务流程。

Oracle Database 11g 切底改变了具有前瞻视野的公司对于数据库平台的需求。由于 Oracle Database 11g 企业级网格运算,各企业现在可以毫无羁绊地追求创新。

- **增益网格实力**

Oracle 倡导企业网格(enterprise grids),挑战建置和维护企业 IT 基础架构的高昂成本。企业网格运用 Oracle Database 11g 及商用服务器和存储,让各企业能够简化自己的基础架构,进而顺应变革,而非管理昂贵的垂直扩展服务器

孤岛;Oracle 企业网格以最低成本独家提供效能、可用性与基础架构灵活性的绝妙组合。

Oracle 企业网格包括 Oracle Fusion Middleware 可以扩展应用软件、Oracle Real Application Clusters (Oracle RAC 以提供扩展性和高可用性,还有 Automatic Storage Management (ASM)以简化管理基本存储基础架构的工作,并使其自动化。Enterprise Manager Grid Contro 简化企业网格和一体化业务流程的管理,以确保快速、安全而且可靠的服务品质。



- **支持非结构化资料**

Oracle Database 11g 为为存储与获取 XML、数据库中的文件提供固有的支持;可以运用业界标准的 SQL、XML 与档案/资料夹接口,存取 XML 文件。XML 文件可以储存两种格式之一来存取:CLOB,以供非结构化与半结构化文件(例如 MS Word 文件),和对象相关 (Object-relational),以供结构化文件(例如采购订单)。Oracle Database 11g 导入全新的储存方式与索引方法,以供非结构化/半

结构化 XML 文件:二进制(binary) XML 与 XML Index。二进制 XML (Binary XML)大幅提高储存效率,而且可以搭配 XML index,在存取 XML 文件时实现高达 15 倍的性能提升。

XML 只是非结构化资料的范例之一,企业必须管理各式各样的非结构化资料。不同的 \企业需要整合地理空间(geospatial)与多媒体等资料,改善业务能见度与流程。Oracle Database 11g 新增更多业界特定数据类型的支持,例如医药业的 DICOM,供应链的 RFID, 以及工程与许多其它业界的全新 3D 空间数据,通过整合各种类型的信息 ,Oracle Database 11g 帮助您汇集和处理非常大量的非结构化与传统结构化资料,实现真正完善整合的信息平台。

采用广泛接受的在数据库中统一管理结构化与非结构化数据的基础架构,针对存取非 结构化信息一直都存在性能问题。为了解决这个课题,Oracle Database 11g 导入了 SecureFiles,这是适用于 LOB 数据类型的崭新而且更佳的存储基础架构。SecureFiles 能够使 Oracle Database 11g 中 LOB 资料的读写性能等于,甚至超越固有的文件系统存储。此外,SecureFiles 还提供 LOB 数据类型的压缩、非复制以及透明的数据加密。所有运用 LOB 的应用软件与数据类型都直接受患于全新的 SecureFiles LOB's。

- **完善整合的业务分析**

更高业务能见度的需求,不仅要涌盖历史的观点,也要透视企业的现在与未来,需要全新而且越来越动态的信息基层架构。Oracle 采用在数据库引攀中嵌入 OLAP、数据挖掘与统计功能的做法。这种完善的整合可以减少将数据移动到到独立分析引擎的必要性;也降,低了系统复杂性、强化数据安全性,甚至能够真正的实时分析运营资料。

Oracle Database 11g 中业务分析最引人入胜的强化就是立万体结构的物化视图 (Cube-organized materialized views)业务分析通常需要多维查询(multi-dimensional c querying);而多维查询让分析师能够解答度量的问题(例如销售),涵盖各种维度(例如产品、地区、日期)。典型的查询可能是「告诉我去年 1、2 月份牛奶销售量最高的前 5 个地区」。通常有两种不同的技术做法可以执行多维查询:以关系型数据库中的星形模型为基础的 SQL 查询,和以 Oracle Database 11g 与 Hyperion Essbase 等 OLAP 服务器中的立方体(cubes)

为基础的 OLAP 查询。很多开发人员和工具都知道如何使用和产生业界标准 SQL，这就是 SQL 做法的优势。OLAP 的优势在于 SQL 开发人员必须建立数百个物化视图，才能达到媲美 1 个 OLAP 立方体的性能水准。Oracle Database 11g 拥有突破性的技术，首度使这两种， 技术一致化，兼得两者的优点。由于 11g 的立方体结构的物化视图(Cube-organizea materialized views)，数据库中的 OLAP 立方体可以扮演星形模型背后的物化视图的角色。现在执行多维查询的数据库应用软件与工具(例如 Oracle EBS、Oracle BI EE Cognos、 Business Objects)等，全都受惠于高性能 OLAP 立方体。

Oracle Database 11g 不断地强化自己的业 界顶尖数据整合工具 Oracle Warehouse Builder，以加速抽取、加载和转换资料，让客户 能够更及时地分析和获得更精确的资料。全新 11g 具备了从 Siebel 应用软件抽取数据的完善整合支持。

- **信息生命周期管理**

信息生命周期管理(Information Lifecycle Management ，ILM)是在 Oracle Database 之下大幅降低存储成本，同时维系服务品质于不下降的好方法。传统的做法是将所有数据库的数据放在单一高效存储层中；这种方法通过 ILM，将数据库的数据放置在多重存储层中：随着数据益趋陈旧而越变越不活跃，然后转放在更低成本的存储介质中。 Oracle Partitioning 让您非常容易就能够在数据库中实现 ILM。例如，假设我们现在是日历年的第三季(Q3)，我们要按月分区订单(Orders)数据以供订单输入应用软件使用。高性能存储层存储经常存取的所有资数据，各分区容纳要储存的 Q3 的订单，这一层使用高性能存储设备。低成本存储层存储比较不常用的资料，各分区容纳 Q1 与 Q2 的订单；这一层使用非常低成本的存储技术，例如 SATA 磁盘阵列。在线归档存储层存储非常少用或修改的所有数据，各分区容纳去年的订单。

Oracle 提供信息生命周期管理(Information Lifecycle Management，ILM) Advisor， 帮助您制定生命周期策略、估计节省的存储成本，并建立转移、归档和删除数据的脚本。

- **性能**

Oracle Database 11g 在性能方面有许多突破。全新的服务器与客户端结果

缓存(result caching 提高经常重复的程序的性能达 25%以上;崭新的内置 PL/SQL 与 JAVA 编译器(native compilers for PL/SQL and Jawa 大幅提高性能,针对 PL/SQL 提高达 2 倍而针对 Java 高达 11 倍;

Oracle Real Application Clusters (Oracle RA 性能针对某些工作 负载提升达 70%,远胜过旧版软件;Oracle Automatic Database Diagnostic Monitor (ADDM)经过强化,可以自动诊断 Oracle RAC 环境中的性能问题。

在其它领域也有许多性能强化,Oracle Streams 快 2 倍,而 optimizer statistics gathering 更快速而且更精准。

最后,如前所述,运用全新的分区方法与立方体结构的物化视图,许多商业智能应用软件的速度提升都很明显。

管理变更的绝佳能力

Oracle Real Application Clusters 与 ASM 等创新而实现的灵活的基础架构具备了变更的能力,但是不一定保证变更不会影响到信息基础架构的稳定性。变更或许是实现灵 性的最大障碍,Oracle Database 11g 导入几项全新功能,克服执行变更同时维护稳定性的挑战。

测试针对基础架构变更的能力 - 例如硬件变更、软件升级与补丁 - 一直都是变更保证的基石。在进入生产环境之前能够测试变更及其影响,的确让人安心不少。许多企业运用仿真软件,企图测试变更的影响,但是还有许多问题没有浮上台面,因为现有的工具无法运用生产等级的工作负载而严格地执行压力测试。

Oracle Database 11g 导入 Real Application Testing,包含两大功能。第一项称为, Database Replay,通过捕获实际的生产数据库工作负载,包括准确的时机、一致性与交易特性,变更后在测试环境中重演。 Database Replay 能够分析和报告所发现的任何差异, 例如性能改善或退化、数据差异,当然还有错误。与仿真测试软件截然不同的是,Real Application Testing 不必开发仿真工作负载或脚本,您可以缩减测试负载,还可以提高信心。

透过 Oracle Data Guard,也可以更轻松地维护测试环境。Oracle Database 11g 导入全新的 Data Guard 功能,称为 Snapshot Standby Data Guard 是灾难恢复工具,也常用来建立生产数据库的只读实例,以供产生报告和备份使用。在 Oracle Database 11g 中 , Data Guard 备份数据库可轻易地转换到 Snapshot

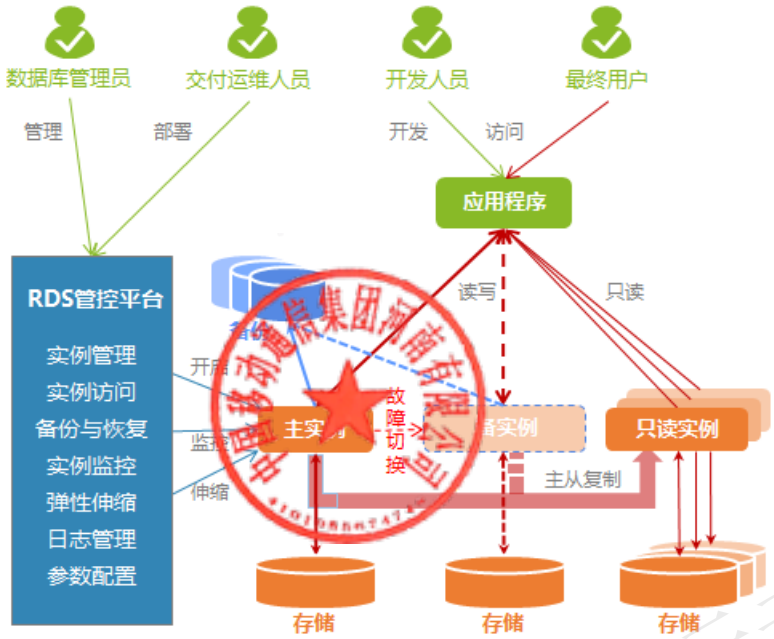
Standby 以供测试。转换到 Snapshot Standby 之后,测试实例就会开放完整的读写功能,并能够执行 Database Replay 捕获的工作负载。绝对不会在测试时遗漏生产时发生的任何变更,因为 Data Guard 会将所有变更纳入队列,并在测试完毕后使备份数据库与生产数据库同步。结果,不仅您可以获得真正的变更保证,还可让备份基础架构的效用发挥到极致。

Real Application Testing 选项的其它功能还有 SQL Performance Analyzer,这项功能能够捕获生产系统的 SQL 工作负载,包括计划与执行统计,还能在变更的测试实例上重现工作负载。SQL Performance Analyzer 能够依据执行计划来报告任何变更,并显示变更后,哪些语句速度变快了,哪些语句速度变慢了。管理人员在 Enterprise Manager 中按下鼠标,就能够传送还原的语句到数据库既有的 SQL Tuning Advisor ,以供后续分析。SQL Tuning Advisor 包含在 Enterprise Manager Tuning Pack 中。

3.2.3.7.3 SQL Server 数据库服务

Microsoft SQL Server 是全球最受欢迎的商用数据库之一。华为云 SQL SERVER 继承了它强大的数据库服务能力，兼容 Windows 系统上的所有应用，同时又拥有云上数据库的所有优良特性：即开即用，稳定可靠，安全运行，弹性伸缩，轻松管理，经济实惠。数据库上云后，你将摆脱传统的运维工作，让你更加专注业务发展。基本工作架构和功能如下：。基本工作架构和功能如下：

公共资源交易平台投标专用
AE2C19CE7C16D1A62A82C88EA14DB9



- **超高性能**：华为云 SQL Server 实例采用最适合数据库服务器的硬件设置进行配置，并针对服务器实例上的 Windows 系统进行 200 多项最佳实践，针对 SQL SERVER 进行 30 多项最佳实践，针对 74 项参数值进行分规格分版本差异化配置，平均性能超友商 1.5X，给你最佳的云数据库服务体验。
- **超高安全**：通过工信部可信云认证，VPC 安全组、数据加密、SSL 加密、防注入攻击和数据库审计，帮你打造全方位的安全服务，并集成世界前 3 数据库安全服务，安全细致到密码设置都是防黑客人体工程学的。
- **超高可靠**：集成商用数据库事务强一致性；云存储 9 个 9 个可靠保证；能让你还原到 5 分钟前任意数据库事件状态节点，并能持续存储 732 天超长备份周期。
- **超高性价比**：支持从 2008R2 到 2017 所有版本，并提供 Web 版，标准版，企业版供用户选择，其中 Web 版开源的价格商用的服务。

3.2.3.7.4 Redis 缓存数据库服务

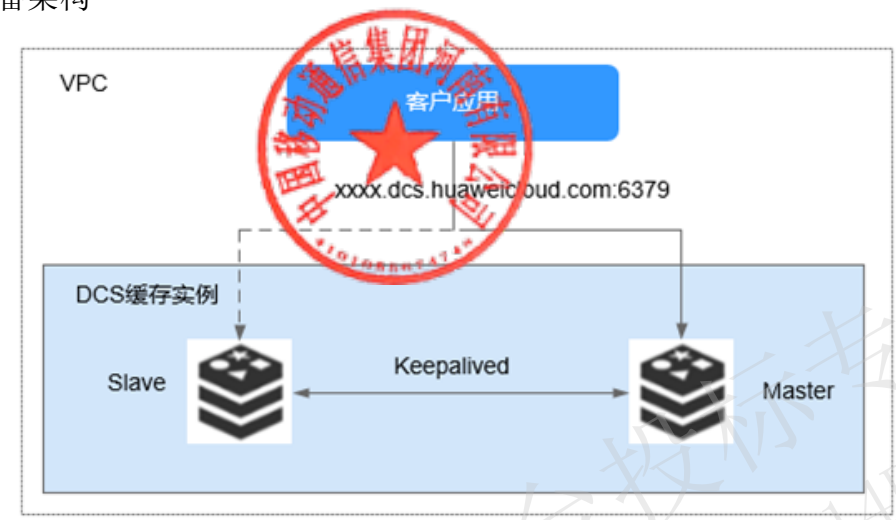
（一）系统架构

公共资源交易平台会员标专用

分布式缓存服务 Redis 是华为云提供的一款内存数据库服务，兼容 Redis 内存数据库引擎，为您提供即开即用、安全可靠、弹性扩容、便捷管理的在线分布式缓存能力，满足用户高并发及数据快速访问的业务诉求。

本项目提供主备架构，集群架构。

1.主备架构



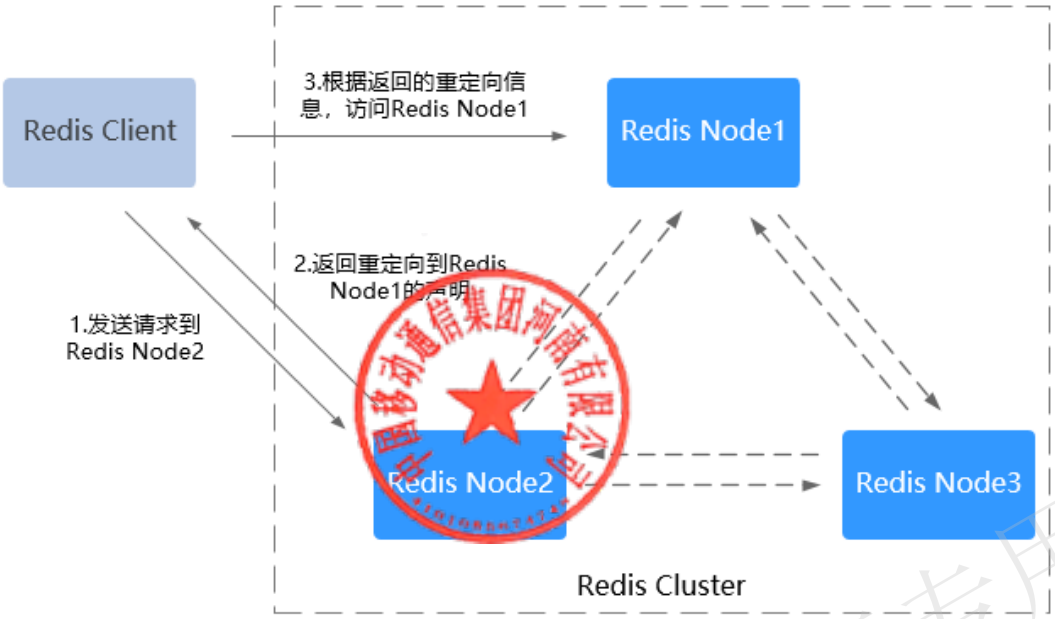
DCS主备架构

- VPC：虚拟私有云。实例的内部所有服务器节点，都运行在相同VPC中。
- 客户应用：运行在ECS上的客户应用程序，即Redis的客户端。Redis实例兼容开源协议，可直接使用开源客户端进行连接。
- DCS实例。主备实例包含了Master和Slave两个节点。默认开启数据持久化功能，同时保持节点间数据同步。
- DCS实时探测实例可用性，当主节点故障后，备节点升级为主节点，恢复业务。
- Redis的访问端口默认为6379。

2.无中心集群架构

Redis Cluster 的任意节点都可以接收请求，但节点会将请求发送到正确的节点上执行，同时，每一个节点也是主从结构，默认包含一个主节点和一个从节点，由 Redis Cluster 根据选举算法决定节点主从属性。

公共资源交易平台投标专用

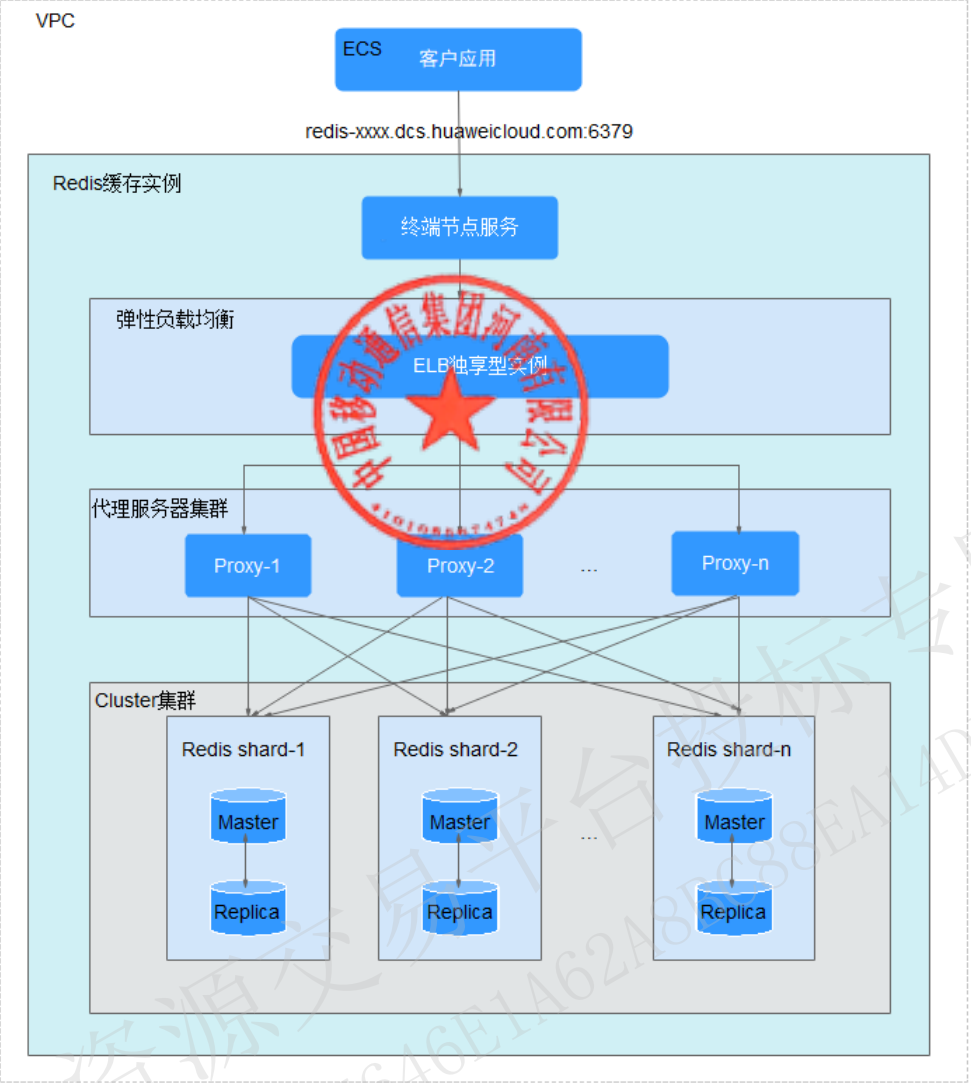


DCS集群架构（无中心）

3. DCS Proxy 集群架构

Redis Proxy 集群实例提供 2G~1024G 多种大容量规格版本，用于满足百万级以上并发与大容量数据缓存的需要。Redis 集群的数据分布式存储和读取，由 DCS 内部实现，用户无需投入开发与运维成本。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88E214DB9



DCSproxy集群架构

VPC

虚拟私有云。集群实例的内部所有服务器节点，都运行在相同 VPC 中。

客户应用程序

客户应用程序，即 Redis 集群客户端。

Redis 可直接使用开源客户端进行连接。

终端节点服务

终端节点服务，主要是将 Redis 缓存实例配置为 VPC 终端节点支持的服务，用户可以直接通过终端节点服务的地址访问。Redis Proxy 集群实例提供的 IP 地址和域名，即为终端节点服务的地址。

ELB

公共资源交易平台商标专用

弹性负载均衡服务器，采用集群高可靠方式。

Proxy

Redis 集群代理服务器。用于实现 Redis 集群内部的高可靠，以及承接客户端的高并发请求。

Redis 集群的分片。

每个分片也是一个双副本的 Redis 主备实例，分片上的主实例故障时，系统会自动进行主备切换，集群正常提供服务。某个分片的主备实例都故障，集群可正常提供服务，但该分片上的数据不能读取。

（二）服务能力

分布式缓存服务 Redis 提供以下主要功能：

1. 即开即用

提供单机、主备和集群三种类型的缓存实例，拥有从 128M 到 1T 的丰富内存规格。您可以通过控制台直接下单购买并创建，无需单独准备服务器资源。

2. 安全可靠

借助华为云统一身份认证、虚拟私有云、云监控与云审计等安全管理服务，全方位保护实例数据的存储与访问。灵活的容灾策略，主备/集群实例从单 AZ（可用区）内部署，到支持跨 AZ 部署。

3. 弹性伸缩

提供对实例内存规格的在线扩容与缩容服务，帮助您实现基于实际业务量的成本控制，达到按需使用的目标。

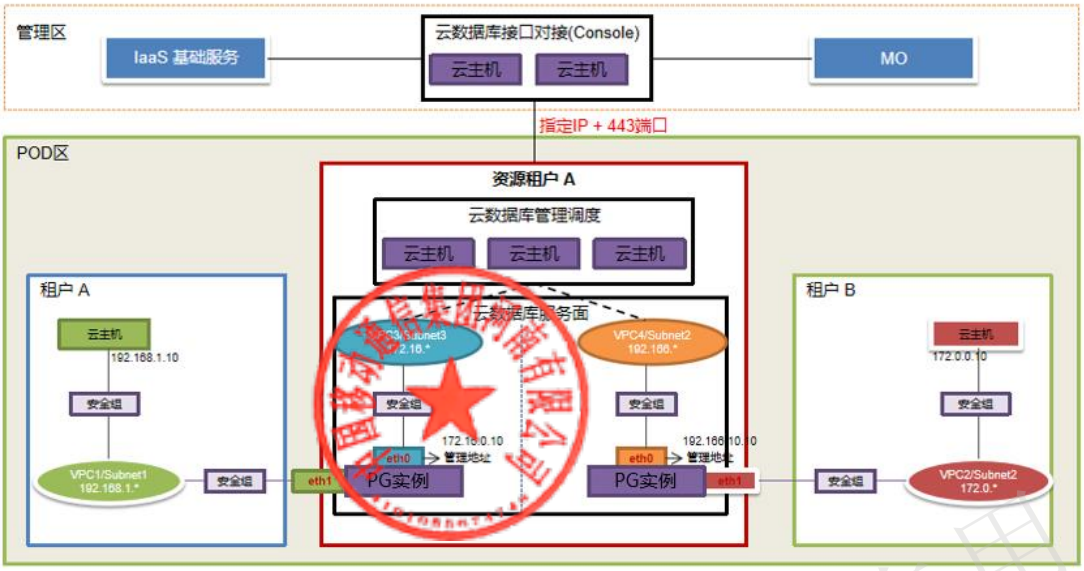
4. 便捷管理

可视化 Web 管理界面，在线完成实例重启、参数修改、数据备份恢复等操作。提供基于 RESTful 的管理 API，方便您进一步实现实例自动化管理。

3.2.3.7.5 PostgreSQL 数据库服务

PostGres 云数据库产品，兼容社区开源版本， 支持 NoSQL 数据类型（JSON/XML/ hstore），支持复杂查询 SQL 的 OLTP 业务场景，提供 PostGIS 地理信息引擎、多维多模时空信息引擎。详细架构图如下：

公共资源交易平台投标专用



- 基本功能

提供统一的前端 web 页面，通过表单创建指定的数据库版本，cpu 内存规格，数据空间、备份空间创建数据库集群。

支持修改实例集群规模。

支持修改实例计算/存储规格。

- 监控告警

采用 promethues+exporter 的架构，通过 RDS exporter 组件，定期采集数据库实例运行过程的指标，将采集后的指标存储到 promethues 集群进行存储

- 日志监控

采用 elasticsearch+fluen-bit 的方式采集和存储日志数据，其中 fluent-bit 组件会监听所有节点的标准容器镜像输出目录/var/lib/containers/*.log，将数据封装成 json 格式存储到 elasticsearch

- 租户管理

集群管理员可配置不同租户，不同租户之间申请的资源相互隔离。

集群管理员可租户配额，配额包括租户可用 CPU、内存和 IOPS。

- 高可靠故障自动切换

当实例所在机器不可用时，数据库实例自动完成主、备的切换，无须人工干预。同时提供手动迁移功能，可手动迁移到其它机器，平台界面化迁移功能，可指定机器来迁移，迁移时会在指定机器创建一个新的实例，待新的实例正常后，

公共资源交易平台技标专用

再删除原来旧实例

Postgre 数据库主要有以下特点与显著优势：

- 云原生特点

基于云原生理念设计，可轻松实现与不同云基础设备资源兼容，快速提供 Postgre 数据库实例服务

- 完整的数据库私有云架构

可实现 PostgreSQL 数据库的创建、使用、调整、监控、回收可以做到整个流程可控，实现 IT 资源的全生命周期管理。

- 双重高可靠架构

在依托 IaaS 底层的计算层、网络层、存储层全冗余的架构设计，实现计算层、互联层、存储层无单点故障的同时。在数据库 PaaS 层又具备了数据库实例级别的高可靠主、备容灾能力，数据库实例支持多 1 主多从多备部署，主备数据库实时自动秒级接管。

- 灵活的扩展性

在底层计算、存储运行资源层面，无论采用任何一种 IaaS 平台和标准的 x86 服务器，容器化原生的分布式特性均能快速的进行在线的弹性扩容，支持读性能可定制。

在数据库实例级别可快速进行数据库集群实例的扩容，当数据库读压力增大以后，可以增加读库，进行数据库读写分离，读性能可线性扩展。

数据库支持一键扩展和一键缩减，读性能伸缩性强。

- 简化运维

在数据库私有云中，数据库性能可以被集中监控和管理。通过将平台管理软件可对运行在平台上的 PostgreSQL 数据库进行有效的统一运维监控和资源限制，降低运维成本，提高业务的连续性。

- 被集成能力

平台具有标准的 API 服务接口，可与第三方云管理平台，实现统一门户集中管理，包括用户、计费、监控等功能对接。

- 高性能

经过深度与主流 IaaS 厂商的适配和优化，Postgre 数据库平台能充分发挥

公共资源交易平台技术专用

IaaS 资源计算与存储的性能，在实现统一监控管理运维外，还能保证数据库的性能。

- 高效、低成本交付模式

平台建设软硬件投入成本低，一键安装部署极其简单。

专业的数据库平台技术服务团队，实现对数据库平台的整体搭建和后续统一的服务支持

快速响应，定期巡检，保证系统的长期稳定运行

- 灵活的部署形态

基于云原生架构的数据库解决方案，是云计算中 PaaS 层的产品，能够部署支持多样的部署形态，可以是物理机裸金属环境的部署，也可以几乎所有 IaaS 基础架构之上部署，另外也支持在任意公有云或混合云的容器云平台上进行部署。

- 可移植性和持续交付能力

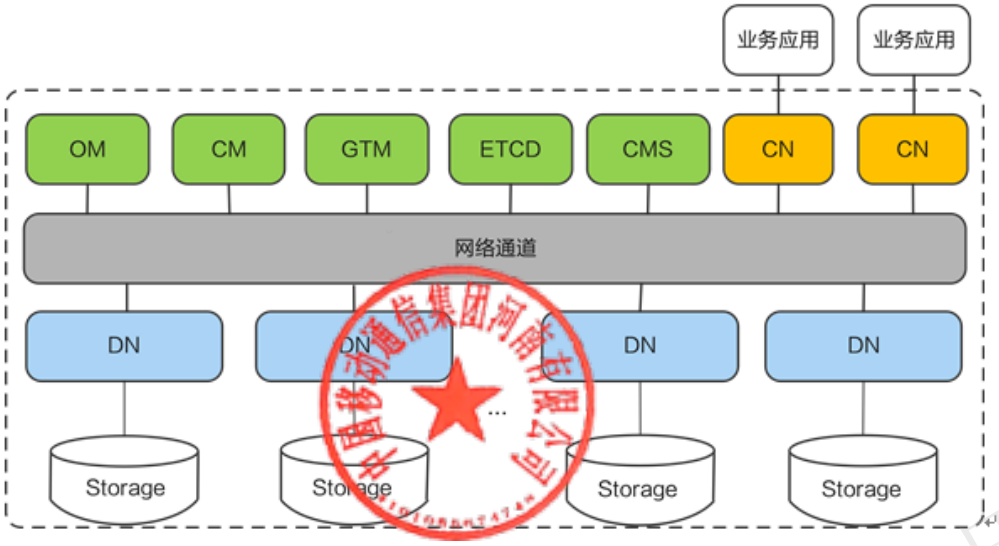
平台基于容器化的“镜像一次构建，可以到处运行”的特点，可轻松进行跨平台性迁移。同时使用构建开发、测试、生产环境变得简单和统一，为用户应用快速跌代持续交付提供数据库服务的基础支撑，具有 CI/CD 持续集成、持续交付和持续部署的能力。

3.2.3.7.6 分布式关系型数据库服务

GaussDB 是华为公司自主研发的新一代企业级分布式关系型数据库，基于 Shared-Nothing 架构，同时支持 x86 和鲲鹏计算架构，提供高吞吐强一致性事务处理能力、金融级高可靠能力、分布式高扩展能力、大数据高性能查询能力，应用于金融、电信、政府等行业关键核心系统。当前支持主备版、分布式两种部署形态。

（一）系统架构

公共资源交易平台投标专用



华为并行数据库基于 Shared-nothing/MPP 架构，面向开放 x86 和华为鲲鹏平台，数据跨所有节点均匀分布，所有节点以并行方式工作，提供标准 SQL 接口，支持 SQL92,99,2003 标准，支持 JDBC/ODBC 标准接口，提供多达 2048 个物理节点 PB 级数据存储分析的扩展能力。

主要包含以下几个组件：

- CN（Coordinator）：协调节点组件，独立进程，SQL 的统一入口，对外接收客户端 SQL 语句，生成分布式执行计划，下发计划片段到各执行节点，各执行节点返回执行结果到 Coordinator，返回给客户端。主要职责是接收 SQL 请求，生成执行计划，汇聚最终结果。
- DN(DataNode)：执行节点组件，也称之为数据节点，独立进程，SQL 执行计划的执行主体，并存放数据。
- GTM（Global Transaction Manager）：全局事务管理器，独立进程，主要是用于维护分布式系统中全局事务一致性。
- CM（Cluster Manager）:集群管理组件，由两部分组成，一个是 CMServer，一个是 CMAgent，每个主机节点部署一个 CMAgent，CMServer 和 CMAgent 均为独立进程，每个主机节点上部署一个 CMAgent，CMAgent 监控这个节点上的所有资源，包括监控网络状态，磁盘状态等硬件设备，以及 CN 节点，DN 节点，GTM 节点等软件设备的状态，CMAgent 进程每隔一定时间向 CMServer 汇报集群各组件状态信息，CMServer 根据 CMAgent 上报

公共资源交易平台技术专用

的状态信息判断集群资源是否发生故障，在集群发生故障时，能够根据故障类型做出相应的故障处理指令，保证集群自恢复。

- OM（Operation Manager）：安装部署运维，配置管理接口工具，独立进程。

系统业务处理流程：

- SQL 语句业务处理流程：客户端发起 SQL，CN 节点接受 SQL，生成分布式执行计划，CN 节点向涉及 DN 节点下发分布式执行计划，DN 节点执行分片执行计划，向 CN 节点返回执行结果，CN 汇聚最终结果，返回给客户端。
- 集群启停业务处理逻辑：cm_ctl 客户端工具发起集群启停命令，CMServer 接受客户端工具发起的命令，将命令下发给各节点，执行启停命令。
- 集群状态查询业务处理逻辑：cm_ctl 客户端工具发起集群状态查询命令，CMServer 返回给客户端工具各节点状态信息。

（二）服务能力

- **高速并行加载**

数据并行导入（加载）的核心思想是充分利用所有节点的计算能力和 I/O 能力以达到最大的导入速度。GaussDB 的数据并行导入实现了对指定格式（支持 CSV/TEXT/FIXED 格式）的外部数据高速、并行入库。

高速、并行入库是和传统的使用 INSERT 语句逐条插入的方式相比较，入库性能得到提升。原理是，并行导入过程中：

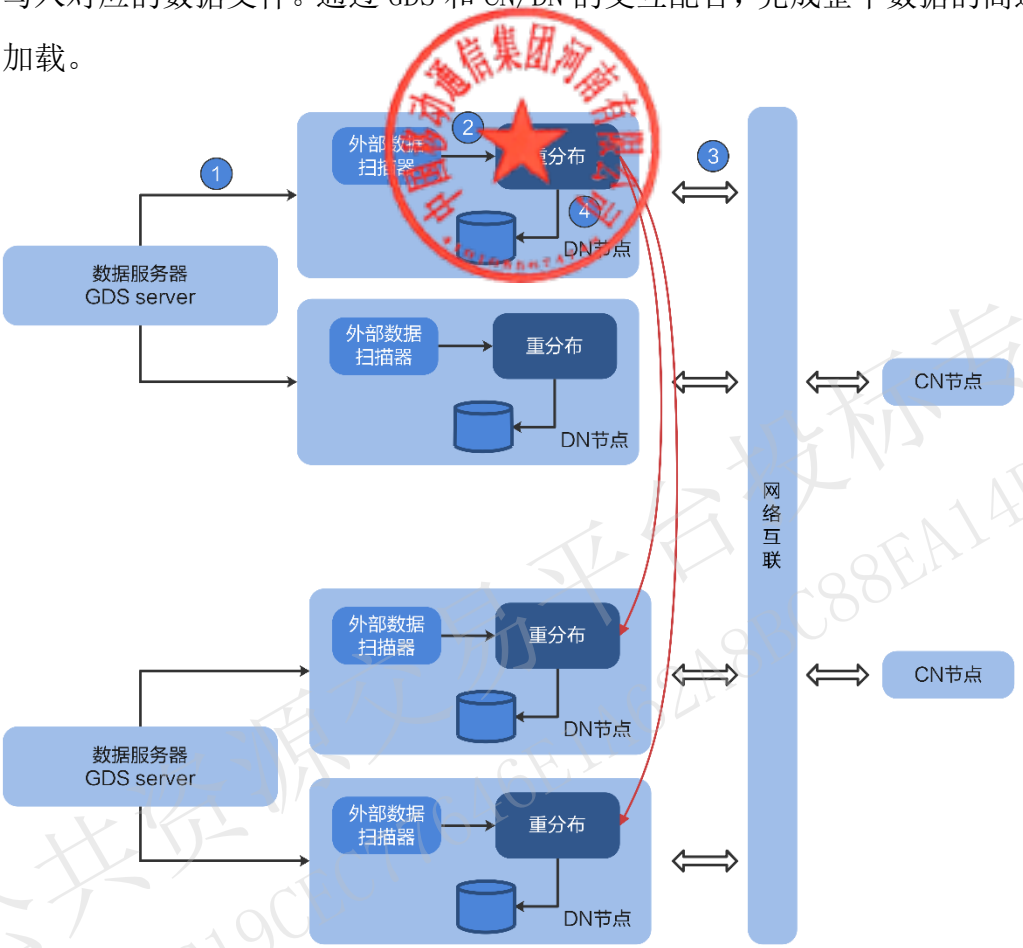
CN 只负责任务的规划及下发，把数据导入的工作交给了 DN，释放了 CN 的资源，使其有能力处理外部请求。

各个 DN 都参与数据导入的工作，充分利用各个设备的计算能力及网络带宽，提高数据导入的整体性能。

以 Hash 分布策略为例介绍 GaussDB 的数据导入过程。数据并行导入的流程图请参见下图。在数据库中创建内表和外表，内表指定 HASH 分布列，外表指定数据源。启动导入数据后，GDS（Gauss Data Service）根据外表指定的数据源

公共资源交易平台投标专用
AE2C15CE27646E1A62A8BC88EA14DB9

将数据分割成固定大小的数据块，发给每个数据节点。各个数据节点并行地处理数据块，每解析出一条数据元组就根据其分布列计算出来的 Hash 值判断存储的物理位置。如果 Hash 在其他网络节点，则需要通过网络重分布到目标数据节点，而如果 Hash 在本地节点，则存储在本地数据节点。数据到达 Hash 所在的节点后写入对应的数据文件。通过 GDS 和 CN/DN 的交互配合，完成整个数据的高速并行加载。

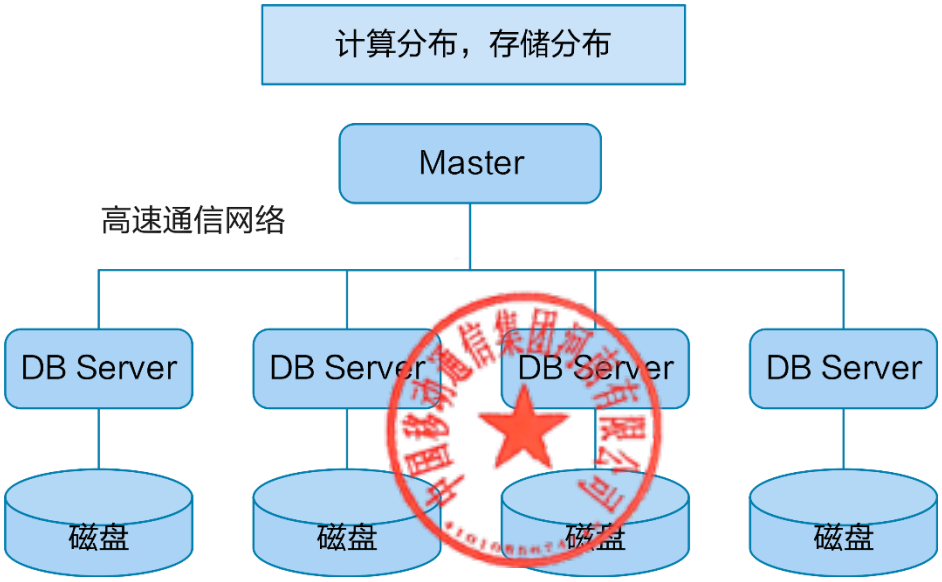


- **全并行分布式执行**

GaussDB 采用 MPP (Massively Parallel Processing) 架构，该架构的特点是：任务并行执行，数据分布式存储(本地化)，分布式计算，私有资源（CPU、内存、磁盘、网络等），可横向扩展，Shared-Nothing。因此 GaussDB 天然具备大规模并行数据处理的能力。

在 MPP 架构的基础上，GaussDB 又增加了 Streaming 流式计算框架，增强了所有计算节点之间的数据交换能力。目前数据库几乎所有的操作都可以实现全并行分布式执行，例如数据扫描、表连接、数据聚合等。且 GaussDB 支持最大 128 个分片的横向扩展能力，其计算能力相比于传统数据库有着巨大的优势。

中国移动通信集团河南有限公司
公共资源交易平台授权专用



- **SMP并行执行**

GaussDB 的 SMP 并行技术是一种利用计算机多核 CPU 架构来实现多线程并行计算，以充分利用 CPU 资源来提高查询性能的技术。

现代计算机体系结构不断朝着多核、大内存等方向发展，一台机器的 CPU 可以有几十甚至上百 core。为了更好的利用 CPU 资源，在大数据分析领域获得更好性能，查询的并行执行技术已经成为现代数据库管理系统的必要组成部分。数据库不仅需要 MPP（Massively Parallel Processing）并行技术做到很好的水平 scale-out（横向扩展），同时也需要支持 SMP（Symmetric Multi-Processing）并行技术在单机上实现更好的 scale-up（纵向扩展）。SMP 可以从两个方面提升数据库的性能，一方面，SMP 可以显著减小单个查询的执行时间，从另一个角度看，SMP 可以提升相同时间段内系统的 throughput，从而有效提升系统资源的利用率。

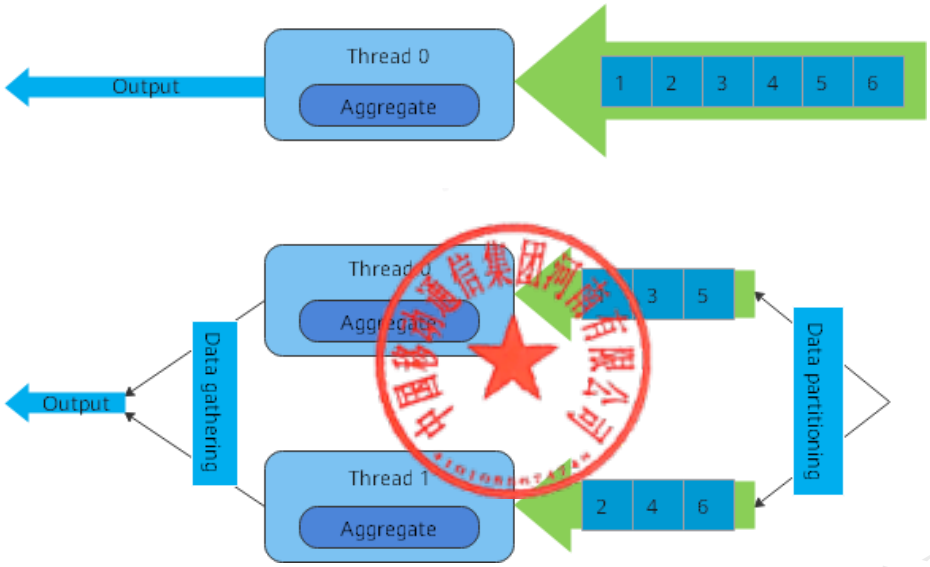
SMP 并行技术通过多线程多子任务并行执行的机制实现系统计算资源的充分高效使用。显然 SMP 多线程轻量执行的模式无疑能够解决 MPP 架构部署上的不足。

首先，SMP 并行执行是在线程级别上来完成任务的并行执行，理论上是可以使并行执行的子任务数达到物理服务器核数的上限。

其次，SMP 并行线程是在同一个进程内，可以直接通过内存进行数据交换，不需要占用网络连接与带宽。降低了限制 MPP 系统性能提升的网络因素的影响。

最后，由于并行子任务启动后不需要附带其他后台工作线程，这样可以增加

系统计算资源的有效利用率。



- **数据生命周期管理-OLTP表压缩**

OLTP 表压缩是 GaussDB 高级压缩中的一个特性，基于全新的压缩算法、细粒度的自动冷热判定和支持块内压缩等技术创新，可以在提供合理压缩率的同时大幅度降低对业务的影响、增加后台调度、增加查询 Job 执行状态以及节约空间。用户可给数据对象指定 ILM 策略，策略分三部分：动作、条件、范围、XX 天未修改条件、行范围。指定策略的表会在后台定时调度、评估表中的每一行是否满足条件，若满足条件则执行行压缩动作。本方案有如下特点：

- 冷热分离

  本方案仅针对冷数据进行压缩，针对热数据的增删改查可以做到无任何影响和额外开销。针对冷数据的删改无任何额外开销（AStore），仅仅影响冷数据的查询（冷数据查询几率较小）有轻微开销，而冷数据的查询几率较低进而可以认为无任何影响。

- 压缩算法

  本方案使用改进版的 LZ4 算法可进一步降低冷数据点查询时的额外开销。该算法可做到当仅需要从压缩块中查询某一小部分数据时候不需要对整个压缩块进行全部解压即可获得，此算法可大大降低冷数据的点查询情形的额外开销。

- 业务零侵入

本方案冷热分离的判定是以行为单位的，这意味着该方案对于数据分布的要求最低，不依赖如多数据源、水平分区、特定的数据分布等其他可见规则，实现业务零侵入。

- 代码低侵入

本方案设计为页内压缩，压缩后的数据与热数据保留在同一空间内，不使用独立的存储结构。且不改变 TupleMeta 部分涉及可见性、锁、事务功能等无影响。对现有堆表引擎修改较少，主要涉及获取 Tuple 的 LastModifiedTime、Select 冷数据适配、Vaccum 冷数据适配以及 Page 内压缩接口。其他的关于后台调度等通过 DEB_SCHEDULE 与 PLSQL 结合完成对后台代码侵入少，易维护性高。

- 调度可控

本方案设计了多个参数可以使用户对后台调度做到全面控制来的得到对业务的影响降至最低。如可控制后台调度发起的时间窗口、时间窗口内可生产 Job 的频率、单次生产 Job 的数量、单个 Job 本身可承载的最大数据量等，同时特殊时期用户也可手动关闭后台调度。

- 可扩展性

本方案设计思想为若数据对象满足 XX 条件执行 XX 动作。基于此思想设计的框架具有较高的扩展性，后期可扩展为：多久未访问从内存中淘汰、多久未访问进行磁盘压缩、多久未访问进行数据归档、表空间较满时进行数据迁移等。

- **Ustore存储引擎**

GaussDB 新增的 Ustore 存储引擎，相比于 Append Update（追加更新）行存储引擎，Ustore 存储引擎可以提高数据页面内更新的 HOT UPDATE 的垃圾回收效率，有效降低多次更新元组后存储空间占用的问题。Ustore 存储引擎采用 NUMA-aware 的 Undo 子系统设计，使得 Undo 子系统可以在多核平台上有效扩展；同时采用多版本索引技术，解决索引清理问题，有效提升了存储空间的回收复用效率。Ustore 存储引擎结合 Undo 空间，可以实现更高效、更全面的闪回查询和回收站

公共资源交易平台投标专用

机制，能快速回退人为“误操作”，为 GaussDB 提供了更丰富的企业级功能。Ustore 基于 Undo 回滚段技术、页面并行回放技术、多版本索引技术、Xlog 无锁落盘技术等实现了高可靠高可靠的行存储引擎。

- **分区**

在 GaussDB 分布式系统中，数据分区是在一个节点内部对数据按照用户指定的策略对数据做进一步的水平分表，将表按照指定范围划分为多个数据互不重叠的部分。

对于大多数用户使用场景，分区表和普通表相比具有以下优点：

- 改善查询性能：对分区对象的查询可以仅搜索自己关心的分区，提高检索效率。
- 增强可用性：如果分区表的某个分区出现故障，表在其他分区的数据仍然可用。
- 方便维护：如果分区表的某个分区出现故障，需要修复数据，只修复该分区即可。

GaussDB 数据库支持的分区表为范围分区表，列表分区表，哈希分区表。

- 范围分区表：将数据基于范围映射到每一个分区，这个范围是由创建分区表时指定的分区键决定的。这种分区方式是最为常用的，并且分区键经常采用日期，例如将销售数据按照月份进行分区。
- 列表分区表：将数据中包含的键值分别存储在不同的分区中，依次将数据映射到每一个分区，分区中包含的键值由创建分区表时指定。
- 哈希分区表：将数据根据内部哈希算法依次映射到每一个分区中，包含的分区个数由创建分区表时指定。

用户可以在实际使用中根据需要调整建表时的分区键，使每次查询结果尽可能存储在相同或者最少的分区内（称为“分区剪枝”），通过获取连续 I/O 大幅度提升查询性能。

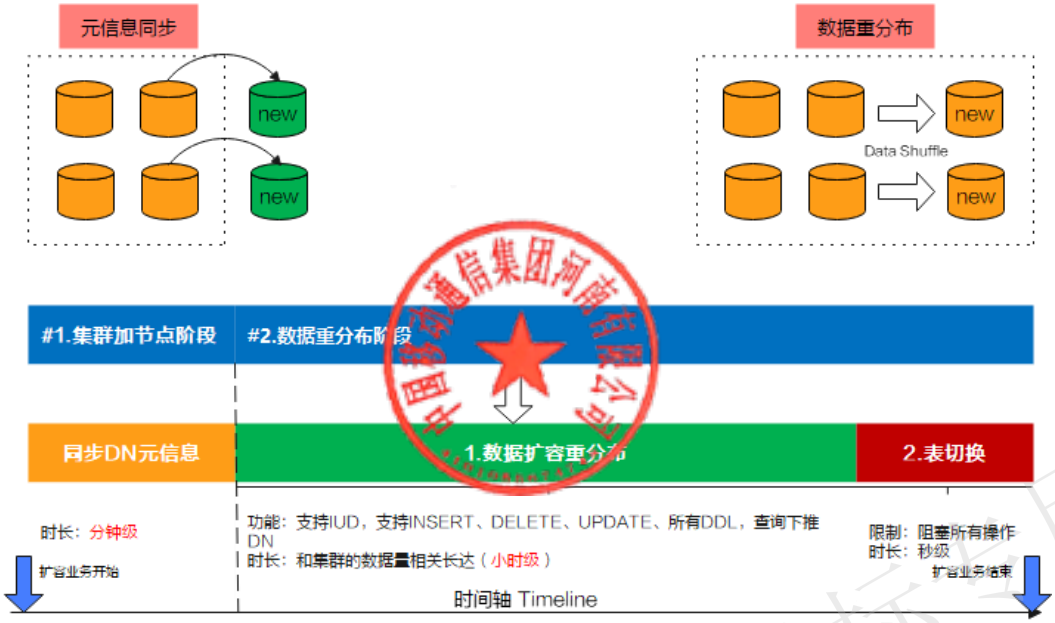
实际业务中，时间经常被作为查询对象的过滤条件。因此，用户可考虑选择时间列为分区键，键值范围可根据总数据量、一次查询数据量调整。

- **在线扩容**

在 OLTP 场景下，随着数据量的增加通常需要对数据库进行扩容。为了保证客户业务在扩容重分布过程中无需中断和平滑过渡，数据库提供在线扩容的能力，设计思路如图 1-2 所示：

公共资源交易平台投标专用

图1-2 在线扩容示意图



在线扩容的原理是集群内众多本地表在不同 NodeGroup 之间的数据搬迁，主要分为集群加节点和数据重分布 2 个阶段。

对于每个扩容重分布的表而言，数据扩容可以分为 3 步：

1. 基线数据扩容重分布
2. 增量数据重分布
3. 表切换

其中第 2 步尤为关键，在此步内，通过行级增量标记技术，来补偿在第 1 步基线数据扩容重分布过程中来自客户业务的并发在线插入、删除和修改。

- **负载均衡**

负载均衡为多 CN 提供一个统一的入口，将客户端的请求均匀的分发给各个 CN 服务器，使系统整体负载均衡。

负载均衡作为集群系统的一个重要组件，承担 2 个职责：

- 均衡各 CN 负载，充分利用多 CN 计算能力。
- 故障隔离，当 CN 故障后，负载均衡能感知故障，并自动停止向故障 CN 节点转发请求。故障感知的时间取决于不同的负载均衡模式，当在内网模式

公共资源交易平台投标专用
AE2C15CEC77646E1A62A8BC88EA14DB9

使用 JDBC client 做负载均衡时，CN 故障感知时间约为 30 秒， 当在外网模式使用 ELB 做负载均衡时，故障感知时间默认为 3 秒(可配置)。

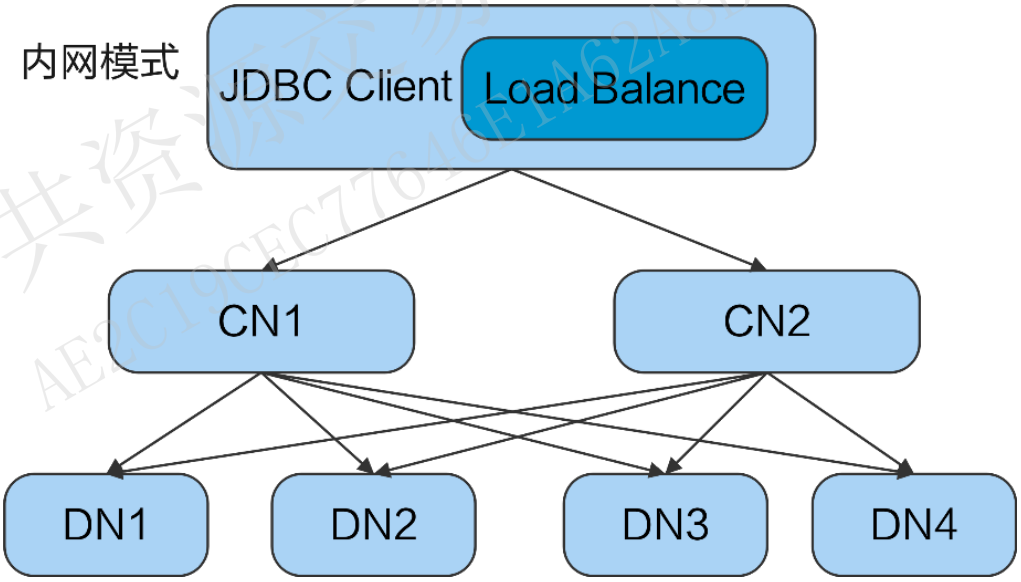
GaussDB 支持 2 种模式的负载均衡：

- JDBC Driver 负载均衡

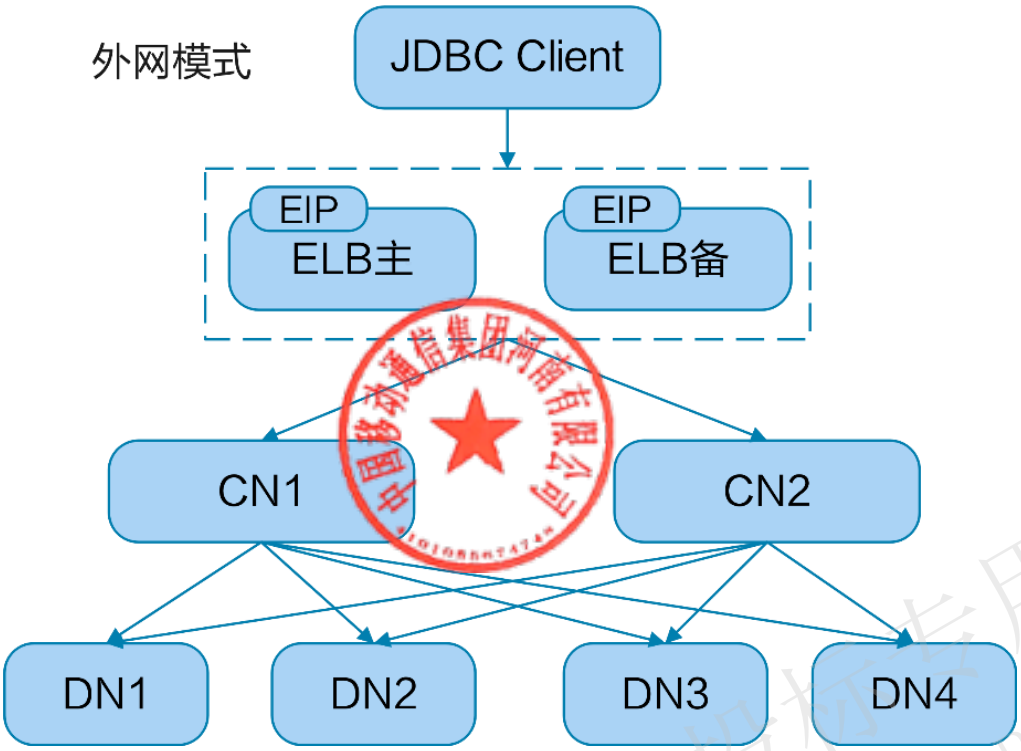
  用户只需在连接串中指定部分 CN，JDBC Driver 从这些 CN 中(高可靠用途)获取所有可用的 CN 列表，然后在这些 CN 列表中进行负载均衡，当某个 CN 故障，将其从可用列表中剔除。刷新可用 CN 列表的时间默认为 10 秒(可配置)。建议用户在使用内网提供服务时使用该模式。JDBC Driver 负载均衡原理如 0 所示。

- ELB 等第三方负载均衡

  GaussDB 支持对接 ELB 等第三方负载均衡方案，建议用户在使用外网提供服务时使用该模式，此时，JDBC Driver 的负载均衡功能可关闭。第三方负载均衡原理如 0 所示。



公共资源交易平台投标专用



- **热补丁升级**

热补丁可以在业务不中断的情况下加载补丁，在不影响业务的前提下，在线解决一部分数据库内核的紧急问题。热补丁基于发布的代码版本生成补丁文件，然后以模块的形式插入到数据库内核运行地址空间中，通过寻找热补丁目标函数的地址，并动态地，原子地替换入口地址，重定向函数代码段至补丁文件代码段达到修复线上系统缺陷的目的。

- 热补丁的制作通过修复特定缺陷函数，制作成模块，动态地加载到运行中的内核系统。
- 热补丁找到目标函数，并在目标函数的入口处加入跳转指令，当目标函数被调用时，跳转到补丁区执行补丁函数
- 目标函数的替换和还原是原子地操作 CPU 寄存器，热补丁可以随时随地加载和卸载，线上系统无需中断，即随时可运行最新的代码

应用价值：

热补丁最大的优势是业务零中断加载补丁，在不影响业务的前提下在线解决一部分数据库内核的紧急问题。

其价值主要体现在如下两点：

公共资源交易平台技术专用

- 缩短版本发布时间，紧急问题从版本回归验证轻量化为补丁回归验证，提高了线上紧急问题的响应速度。
- 热补丁的加载，卸载对业务无感知，提高了客户满意度。

- **灰度升级**

灰度升级是一种支持优先升级部分节点的在线升级方式。

灰度升级主要包含以下 3 个方面：

1. 对于大版本升级涉及的系统表变更，将不同版本的系统表结构和系统函数硬编码在二进制中，保证新、老版本二进制均能解析和使用新、老版本的系统表元组；
2. 对于大版本升级和二进制升级涉及的新、老二进制替换，先灰度替换指定节点上的二进制，待系统运行一定时间之后，再替换剩余节点的二进制。灰度升级节点的选择需要满足以下约束：若灰度升级节点全部发生宕机，那么剩余的节点（老二进制）仍可以提供正常的数据库服务，即剩余的节点至少包含每个分片的一个副本（或多数派副本）。
3. 在第 2 点的基础之上，如果升级亦涉及到节点的操作系统、硬件升级（且不能提前执行），那么在灰度升级部分节点之前，先将这些节点上的主实例全部切换到非灰度升级的节点上；如果升级只涉及数据库二进制的替换，为了尽可能降低对于业务的影响，采用同一节点两套二进制同时存在的方式，使用软连接切换的方式来进行进程版本的切换升级（闪断一次，10 秒以内）。

应用价值：

- 支持数据库的大版本升级和小版本升级（内核版本号不变的升级方式为小版本升级，否则就是大版本升级）。

支持在线升级，允许优先升级部分节点，升级节点闪断一次（10s 以内）。

- **动态数据脱敏**

为了在一定程度上限制非授权用户对隐私数据的窥探，可以利用动态数据脱敏（Dynamic Data Masking）特性保护用户隐私数据。在非授权用户访问配置了动态数据脱敏策略的数据时，数据库将返回脱敏后的数据而达到对隐私数据保护的目的。

管理员可以在数据列上创建动态数据脱敏策略，该策略指出针对特定用户场景应采取何种数据脱敏方式。在开启动态数据脱敏功能后，当用户访问敏感列数据时，系统将用户身份信息例如：访问 IP、客户端工具、用户名来匹配相应的脱敏策略，在匹配成功后将根据脱敏策略对访问列的查询结果实施数据脱敏。

动态数据脱敏的目的是在不改变源数据的前提下，通过在脱敏策略上配置针对的用户场景（FILTER）、指定的敏感列标签（LABEL）和对应的脱敏方式（MASKING FUNCTION）来灵活地进行隐私数据保护。

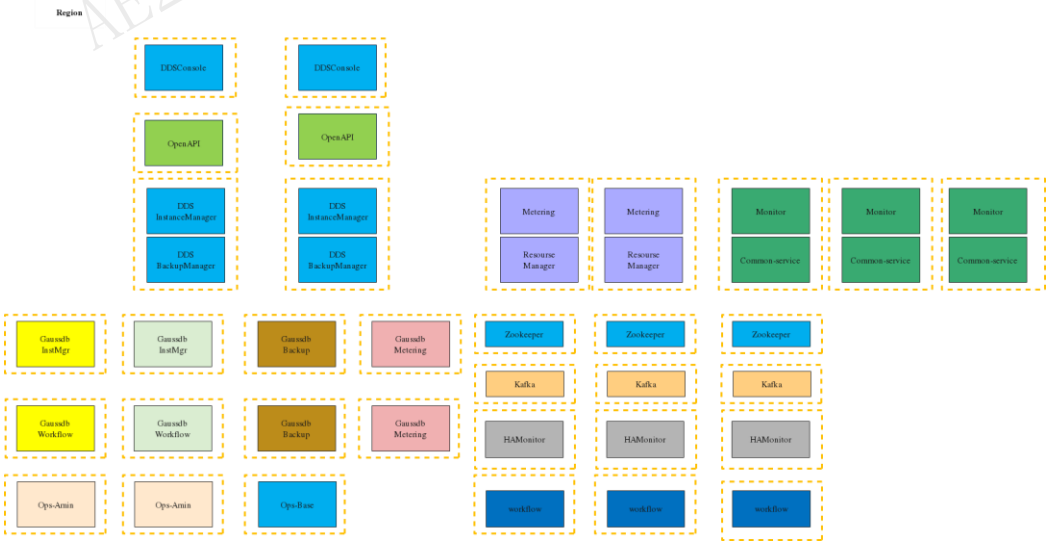
- **数据库监控**

对运行状态和性能指标进行监测是数据库的重要功能。除了对数据库的基本运行状态，例如主机和服务状态进行监控，还需要具备数据库细粒度监控能力。例如业务系统运行缓慢，可能有由于异常行活动导致磁盘争用，并发连接过多导致拥塞，多列/单列统计信息未收集等多种原因。不但需要准确地测量和统计出详细的关键性能指标（Key Performance Index，简称 KPI）数据，还要分析各种数据库活动的运行情况，及时发现其中的异常行为，为用户定位提供参考和建议。

GaussDB 提供了丰富的性能监控数据报表，对数据库的实时运行情况和历史数据进行全面的统计和分析，并通过 WEB 页面直观地呈现给用户。用户可随时查看数据库健康状态指标，以辅助用户快速分析定位各种系统相关问题。

3.2.3.7.7　分布式文档数据库服务

（一）系统架构



每一个虚线框表示一台服务器，存在多个服务部署在同一台服务器上面的情况，各个组件说明如下表所示：

组件名称	组件所在节点	部署状况	部署关系（主备/多活）	网络平面	组件说明
DDS Console (Static)	DBS-console_for_dds01、DBS-console_for_dds02	2 节点部署	多活	DMZ_service	管理面组件，提供可视化页面给用户使用。
DDS API	DBS-api_for_dds01、DBS-api_for_dds02	2 节点部署	多活	DMZ_service DMZ_service_Advance	管理面组件，API 负责提供对外的所有入口，并转发给各个服务执行。
DDS InstanceManager	DBS-mongomgnt01、DBS-mongomgnt02	2 节点部署	多活	DMZ_service DMZ_service_Advance	管理面组件，实例管理负责实例整个生命周期的管理和调度，包括创建实例、重启实例、重置密码、节点扩容、实例删除等功能。

公共资源交易平台投标专用

组件名称	组件所在节点	部署状况	部署关系（主备/多活）	网络平面	组件说明
DDS BackupManager	DBS-mongomgnt01、DBS-mongomgnt02	2 节点部署	多活	DMZ_service DMZ_service_Advance	管理面组件，备份管理负责实例备份/恢复的管理，管理实例的备份策略，提供自动全备、增量备份、备份恢复新实例、PITR 恢复新实例及已有实例等能力。
GaussDB Core	DBS-GaussCore-01、DBS-GaussCore-02	2 节点部署	多活	external_om	管控面核心 Core 元数据库，保存管理面核心数据的数据库。
GaussDB Workflow	DBS-GaussBase-01、 DBS-GaussBase-02	2 节点部署	多活	external_om	管控面工作流元数据库，保存管理面工作流服务状态信息的数据库。

公共资源交易平台投标专用

组件名称	组件所在节点	部署状况	部署关系（主备/多活）	网络平面	组件说明
GaussDB Backup	DBS-GaussBackup-01、 DBS-GaussBackup-02	2 节点部署	多活	external_om	管理面备份服务元数据库，保存管理面备份服务产生的相关数据。
GaussDB Metering	DBS-GaussMetering-01、 DBS-GaussMetering-02	2 节点部署	多活	external_om	管理面计量元数据库，保存计量计费数据。
Ops-Admin	DBS-OpsAdmin-01、DBS-OpsAdmin-02	2 节点部署	多活	DMZ_service DMZ_service_Advance	Region 域运维节点。
Ops-Base	DBS-OpsBase	1 节点部署	多活	DMZ_service	OM 域运维节点。
Metering	DBS-ResMgnt-01、DBS-ResMgnt-02	2 节点部署	多活	DMZ_service DMZ_service_Advance	管理面计费服务，产生话单等计费数据。

公共资源交易平台投标专用

组件名称	组件所在节点	部署状况	部署关系（主备/多活）	网络平面	组件说明
Resourse Manager	DBS-ResMgnt-01、DBS-ResMgnt-02	2 节点部署	多活	DMZ_service DMZ_service_Advance	资源管理服务，和 IaaS 直接交互，提供和 IaaS 交互的接口。
Monitor-Service	DBS-Monitor-01、DBS-Monitor-02、DBS-Monitor-03	3 节点部署	多活	DMZ_service DMZ_service_Advance	实例故障与监控服务，提供实例的状态和错误日志慢日志等实例信息。
Common-service	DBS-Monitor-01、DBS-Monitor-02、DBS-Monitor-03	3 节点部署	多活	DMZ_service DMZ_service_Advance	管理面公共接口服务，提供诸如查询实例个数实例状态等公共接口。
Zookeeper	DBS-Zookeeper-01、DBS-Zookeeper-02、DBS-Zookeeper-03	3 节点部署	多活	external_om	Zookeeper 集群，管理面的注册中心和 Kafka 的仲裁中心。
Kafka	DBS-Kafka-01、	3 节点	多活	DMZ_serv	Kafka 集群，

公共资源交易平台技术专用
AE2C19CEC776A6E1A62A8DC88D142DB9

组件名称	组件所在节点	部署状况	部署关系（主备/多活）	网络平面	组件说明
	DBS-Kafka-02、DBS-Kafka-03	部署		ice DMZ_service_Advance	负责保存实例上报的元数据。
DDS HA	DBS-HA-For-DDS-01、DBS-HA-For-DDS-02、DBS-HA-For-DDS-03	3 节点部署	多活	DMZ_service DMZ_service_Advance	管理面组件，提供实例的高可靠和高可靠能力，包括实例故障拉起、主备倒换等关键能力。
Workflow	DBS-Workflow-01、DBS-Workflow-02、DBS-Workflow-03	3 节点部署	多活	external_om	管理面工作流服务，提供管理面工作流接口。
Agent	各数据库实例	与内核合并部署	-	POD	业务侧组件，负责整个实例的管理，是实例管理、备份、HA 等服务的最终执行者，同时负责

公共资源交易平台投标专用

组件名称	组件所在节点	部署状况	部署关系（主备/多活）	网络平面	组件说明
					实例的各类监控。

（二）服务能力

MongoDB 是基于分布式文件存储的数据库，具有高性能、可扩展、易部署、易使用的特点，存储数据非常方便。除通用特性之外，还支持以下功能特性：

1）支持分片集群、副本集、单节点三种部署架构；

2）支持 MongoDB 3.4、4.0 等版本，满足不同业务系统对数据库版本的需求；

3）支持通过安全组限制源端 IP 对 DDS 的访问权限，可以细化到端口；

4）支持租户使用自己在 KMS 服务上上传的密钥对 DDS 数据进行静态加密；

5）支持库表级时间点恢复，单次恢复支持不同库表选择不同时间点；

6）支持修改连接 IP 和安全组；

7）支持自动和手动主备倒换。

文档数据库服务支持三种部署架构，包括集群、副本集以及单节点实例，满足不同的业务场景。

- **集群**

集群实例提供 mongos、shard、和 config 三类节点。您可以自由的选择 mongos 节点和 shard 节点的个数和配置，组建服务性能不同的文档数据库集群实例。

- **副本集**

文档数据库服务自动搭建副本集架构，您可以直接操作 Primary 和 Secondary 节点。文档数据库服务为您提供高可靠、容灾切换等高级功能，使用过程中对应用完全透明。

- **单节点**

数据库部署在一台虚拟机上，没有高可靠特性。全量备份时为了保证数据一致性，会在备份过程中锁表，备份期间数据不可写。单节点架构成本较低，是研发测试环境、学习培训环境、小型企业内部系统业务等的首选。

弹性扩容

根据业务发展需要，您可以实时变更实例的 CPU 和内存规格、扩容磁盘存储空间、增加 mongos 和 shard 节点数量。同时，建议您尽量选择在业务低峰期进行变更，避免在变更过程中对业务造成影响。

关键功能特性

功能特性	说明
SLA	99.99%
灵活应用	您可以通过控制台实时创建目标实例，配合弹性云服务器一起使用，通过弹性云服务器内网连接文档数据库，有效地降低应用响应时间、节省公网流量费用。通过本地设备访问实例时，可以为其绑定弹性公网 IP，通过弹性公网 IP 连接文档数据库。
完全兼容	文档数据库服务是面向文档型的 NoSQL 数据库，完全兼容 MongoDB 协议。
可视化运维	控制台提供可视化实例管理平台，对实例重启、备份、数据恢复等高频需求实现一键式便捷操作。
数据安全	• 通过虚拟私有云、子网、安全组、存储加密、DDoS 防护以及 SSL 安全访问等多层安全防护体系，有力地抗击各种恶意攻击，保证数据安全。 • 提供审计日志功能，审计日志最长支持保存两年。 • 支持细粒度权限控制。
高可靠	集群和副本集支持高可靠，一旦 Primary 节点发生故障导致节

公共资源交易平台投标专用

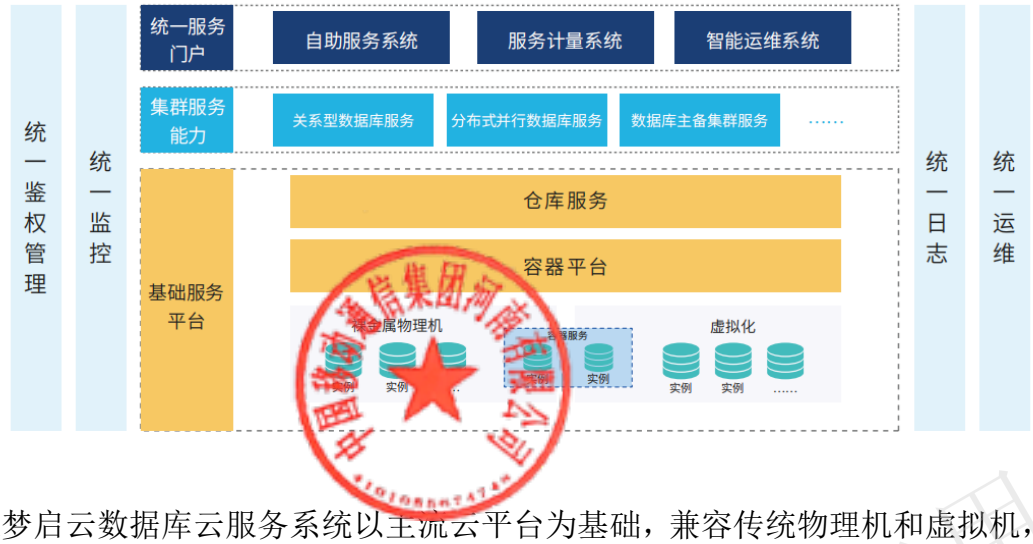
	点不可用，即可在很短时间内切换到 Secondary 节点上，切换过程对应用透明。
指标监控	实时监控数据库实例及引擎的关键性能指标，包括 CPU、内存使用率，磁盘利用率，command、delete、insert 语句执行频率，活跃连接数等指标。
备份与恢复	• 支持设置自动备份策略和实时手动备份。其中，自动备份保留时长最多达到 730 天，实时手动备份长期保留。 • 支持通过备份文件进行数据恢复。其中，副本集支持实例级时间点恢复和库表级时间点恢复。
日志管理	支持查询和下载数据库错误日志和慢日志。
参数配置	控制台支持在线修改并生效配置参数，以及参数组配置管理功能。

3.2.3.7.8 国产数据库

- **达梦数据库**

达梦启云数据库云服务系统是基于自主原创的关系型数据库软件，集数据存储、备份、高可用、迁移、监控、优化、安全等功能为一体，为用户提供一个灵活的、可扩展的、按需申请的数据库服务系统。云服务系统支持多种数据库服务能力，将数据库服务化，开箱即用，并提供并行处理集群、读写分离集群、主备集群等服务能力，可按需适配各种业务场景。

公共资源交易平台投标专用



达梦启云数据库云服务系统以主流云平台为基础，兼容传统物理机和虚拟机，为用户提供自助式的数据库服务，提供全流程的数据库管理及开发体验，由用户管理人员管理和发放数据库实例，开发者及数据库管理员在线上使用数据库，开发者使用数据库服务和使用传统物理机、虚拟机上体验完全一致。达梦启云数据库特点如下：

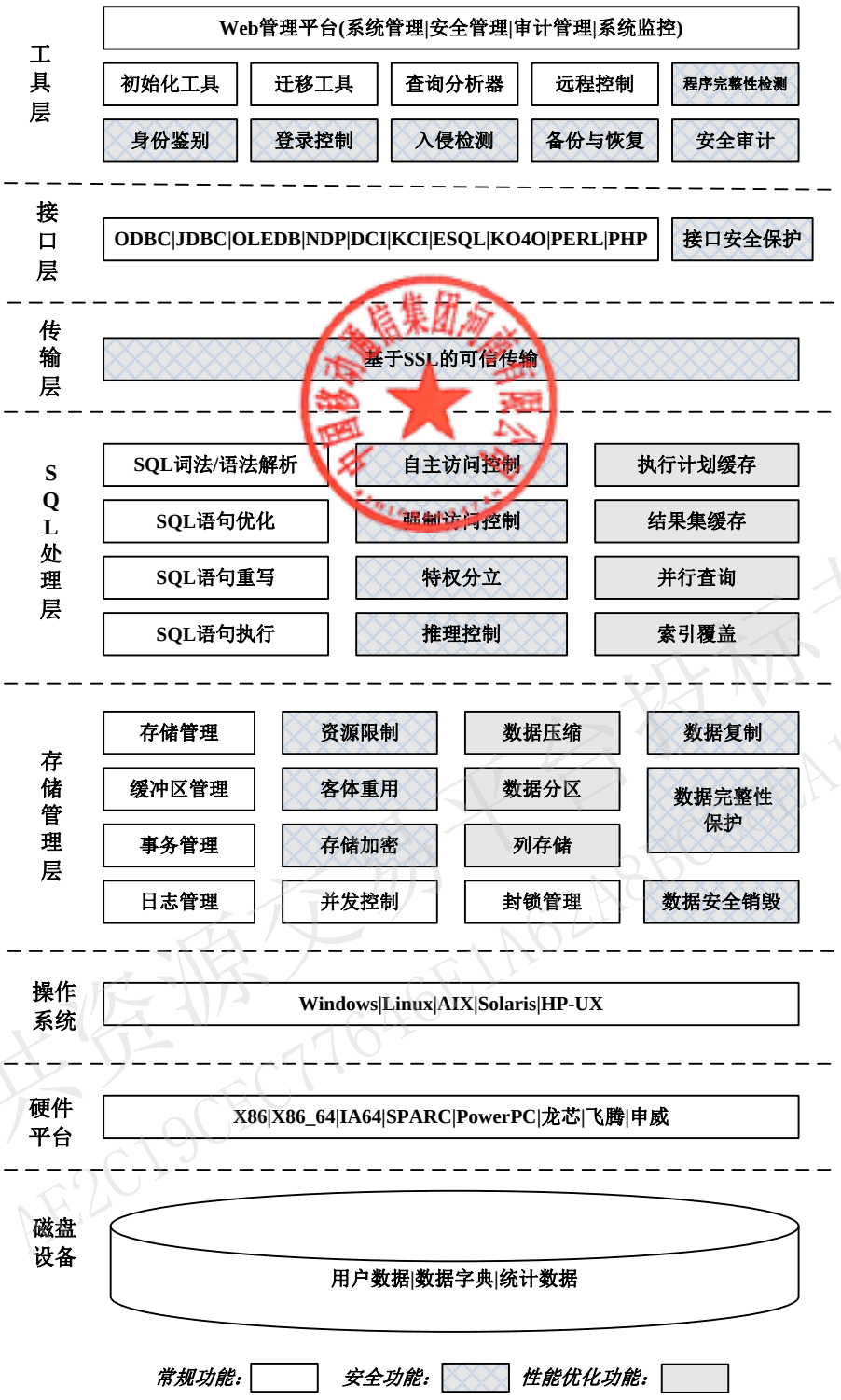
- **自主原创：**采用自主研发的 DM8 关系数据库（包含标准版、企业版、安全版），充分保障数据安全。
- **超融合架构：**采用超融合基础架构，基于低成本实现计算和存储的高可：用，为数据库云服务系统带来最优的效率、灵活性、规模、成本和数据保
- **多样化服务能力：**提供关系数据库、并行处理集群、主备集群、读写分离集群、数据共享集群、图数据库、大数据平台服务能力。
- **自助菜单服务：**用户在统一服务门户上通过服务菜单，自助按需申请数据库服务。
- **智能运维：**系统采用由机器学习算法自动地从海量运维数据（日志、监控信息、应用信息等）中不断地学习，不断优化运：维算法及规则，指挥监测系统采集决策所需的数据，做出分析、决策，实现系统的智能运维。
- **高性能：**数据库云服务系统采用分布式架构，根据用户数据和业务的增长情况而进行数据库的弹性扩展。

公共资源交易平台投标专用

- **高可用：**不会因为单硬盘故障、单个节点故障、单台交换机故障导致业务停顿或数据丢失。
- **多云支持：**支持公有云、私有云、裸金属部署。
- **统一数据管理：**数据库云服务系统支持主流的数据库引擎，能将不同数据库资源整合，提供统一数据库运维平台，实现异构数据库的统一管理。
- **人大金仓 KingbaseES 数据**

KingbaseES 汇集了人大金仓在数据库管理系统领域十几年的技术积累，以及公司在国家重大科技项目“核高基”重大专项数据库课题的研究成果，并在系统的高可靠性、高可用性、高性能、高安全性和高兼容性等方面进行了重大改进。目前共发布了标准版、企业版、安全版、军用版和集群版等版本。这些版本可以满足各种业务场景对通用数据库管理系统的技术需求，并广泛适用于电子政务、军队、电力、金融、教育及交通等行业。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14B29



KingbaseES 数据库功能架构见上图，各个模块按照功能所涉及的逻辑内容分门别类的放到了不同的层级中，如工具层、接口层，SQL 处理层，存储管理层。同时由于数据库所实现的功能是根据这些功能模块相组合来实现的。因此在以下叙述中，根据数据库所实现的功能来描述。在此过程中，会把重要部分所涉及的

模块加以说明。

整体上，金仓数据库 KingbaseES 的技术架构可分为五层，从下到上依次为：

- **存储管理层：**除实现数据存储管理、封锁、并发控制、事务管理、缓存管理、日志空间管理等常规功能外，还提供了如资源限制、客体重用、存储加密和数据安全销毁等安全功能，以及如数据压缩和分区、列存储等性能优化功能。
- **SQL 处理层：**主要负责 SQL 语句（如函数、索引、数据字典、存储过程、触发器）的底层实现。在这一层上，除提供了 SQL 语句的常规处理功能外，还提供了如权限管理和访问控制等在内的多个安全功能，以及如执行计划缓存、结果集缓存、索引覆盖和并行查询等在内的多个性能优化功能。
- **传输层：**提供了基于 SSL(即安全套接层)协议的可信传输方案，以确保用户与数据库服务器间的安全数据交换。
- **接口层：**主要提供各种常见的数据库访问接口及其驱动程序实现，这些常见应用编程接口如 ODBC、JDBC、OLEDB、NDP、DCI、KCI、ESQL、KO4O、PERL 和 PHP。
- **工具层：**主要提供给管理员大量便捷高效的数据库管理工具和开发工具。在此基础上，出于数据库安全考虑，还提供了如身份鉴别、登录控制、入侵检测、安全审计等多个安全保护工具。

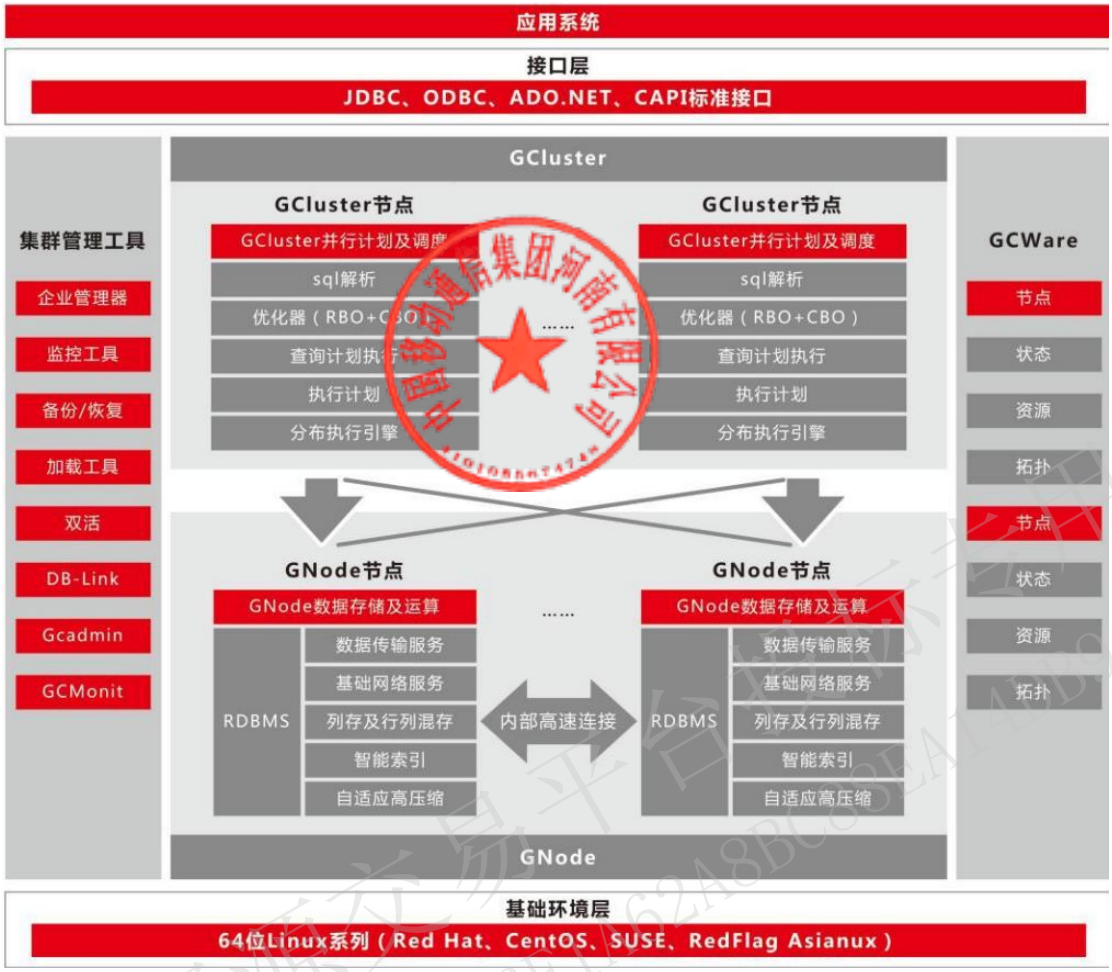
如上图所示，KingbaseES 的安全防护手段和策略贯穿以上各个层次，提供特权分立、访问控制、安全审计、存储加密等多种安全组件和功能，为系统提供了内核级的层层安全防护。不仅如此， KingbaseES 在内核级还实现了多种性能优化，以应对大客户的高负载大并发的业务需求。

- **南大 GBase 8a MPP Cluster 数据库**

南大通用大规模分布式并行数据库集群系统，简称：GBase 8a MPP Cluster，它是在 GBase 8a 列存储数据库基础上开发的一款 Shared Nothing 架构的分布 式并行数据库集群，具备高性能、高可用、高扩展等特性，可以为各种规模数 据管理提供高性价比的通用计算平台，并广泛用于支撑各类数据仓库系统、

公共资源交易平台技标专用

BI 系统和决策支持系统。



GBase 8a MPP Cluster 采用 MPP + Shared Nothing 的分布式联邦架构，节点间通过 TCP/IP 网络进行通信，每个节点采用本地磁盘来存储数据。实现非对称部署，分布式管理集群和分布式调度集群部署在一个集群；分布式计算 集群部署在另外一个集群。系统中的每一个节点都是相对独立的、自给的，整 个系统中不存在单点瓶颈，具有非常强的扩展性。

由于没有资源共享，增加节点就可以线性地扩展数据容量和计算能力，可 以从几个节点扩展到上百节点，满足业务规模增长的要求。

GBase 8a MPP Cluster 产品总共包含三大核心组件，分布式管理集群 GCWare、分布式调度集群 GCluster 和分布式存储计算集群 GNode。它们的功能分别为：

GCluster：负责 SQL 的解析、SQL 优化、分布式执行计划生成、执行调度。

GCWare：用于各节点 GCluster 实例间共享信息(包括集群结构，节点状态，

节点资源状态等信息)，以及控制多副本数据操作时，提供可操作节点，控制各节点数据一致性状态。

GNode：是 GBase 8a MPP Cluster 中最基本的存储和计算单元。

GNode 负 责集群数据在节点上的实际存储，并从 GCluster 接收和执行经分解的 SQL 执行 计划，执行结果返回给 GCluster。数据加载时，GNode 直接从集群加载服务接 收数据，写入本地存储空间。采用虚拟集群部署策略时，可以按不同业务特点 将不同节点进行物理隔离，形成不同的 VC。

VC(Virtual Cluster)：实现单个业务的独立管理，包括 database、表等 数据库对象。 Free Nodes （闲置节点）：不属于任何 VC 的 GNode 节点，通常是备机或 待扩容或节点替换的节点。

除了以上核心组件外，还有 GCMonit 组件，用于实时监测 GBase 8a MPP Cluster 服务程序的运行状态， 一旦发现某个服务程序的进程状态发生变化，就会根据配置文件中的内容来执行相应的服务启停脚本命令，从而保证服务程序健康运行。

GBase 8a MPP Cluster 具有联邦构架、大规模并行计算、海量数据压缩、高效存储结构、智能索引、虚拟集群及镜像、灵活的数据分布、完善的资源管 理、在线快速扩展、在线节点替换、高并发、高可用性、高安全性、易维护、 高效加载等技术特征，具体如下：

1）**联邦架构：**基于列存储的完全并行的 MPP + Shared Nothing 的联邦 架构，采用多活 Coordinator 节点、运算节点的两级部署结构，避免 了单点性能瓶颈和单点故障。Coordinator 节点支持最多部署 64 个； 单个虚拟集群的数据节点支持部署 300 个以上，包含多个虚拟集群的 同一物理集群数据节点支持部署 1000 个以上；单节点可支持 100TB 裸数据量，且所有节点无共享；集群支持海量数据存储、查询，单个 物理集群支持 100PB 以上的结构化数据；

2）**大规模并行计算：**通过采用 MPP 技术的计划器，基于规则和基于代价 的优化器，基于异步 I/O 技术的调度器，支持高并发、高可靠、大规 模的并行调度；

3）**海量数据压缩存储：**可支持 100PB 以上的结构化数据，采用 hash、random 及 replicate 的分布策略进行数据分布式存储；同时采用先进的压缩

算法、基于列存储的数据编码及高效压缩技术，减少存储数据 所需的空间，并相应地提高 I/O 性能；支持实例级、表级、列级三级压缩；压缩比可达 1:20 以上；

4） **高效存储结构：**采用基于列存储、适合分析优化的存储结构；支持行 列混合存储的存储结构，有效提高列存数据库在 select * 场景下的 查询性能；

5） **智能索引：**采用高性能、免维护的粗粒度智能索引技术，索引建立膨 胀率不超过百分之一。智能索引包含基本列的统计信息，在数据检索 定位时可被直接使用，有效过滤数据，大幅降低数据库磁盘 I/O，大 幅提高海量数据的查询性能；

6） **虚拟集群及镜像集群：**通过虚拟集群技术，可以对集群中的运算节点 进行分组，物理上进行资源的隔离；对命名空间进行逻辑隔离，支持 多租户的使用方式。通过镜像技术，在不同的虚拟集群间对数据进行 复制，提供更高的容灾能力，满足更灵活的系统容灾和读写负载分离 等业务场景需求；

7） **完善的资源管理：**通过资源池及资源使用计划的灵活配置，可以支持 对 CPU、内存、磁盘空间、磁盘 IO、并发任务数等关键资源和指标进 行管控；能够提供完善的多租户能力；

8） **在线高性能扩展：**支持集群节点的在线扩容和缩容，效率更高，对业 务的影响更小；在线扩展性能大于 20TB/小时；

9） **高并发：**读写不互斥，支持数据的边加载边查询，并发能力大于 1000；

10） **数据高可用：**通过冗余机制来保证集群的高可用特性，互备分片间可 实现数据自动同步。数据通过副本提供冗余保护，数据的副本机制支 持 1 或 2 个数据副本，支持用户自定义的数据副本分布方式；自动故 障探测和管理，自动同步元数据和业务数据，副本故障不影响集群的 可用性，支持故障的自动恢复，无需人工干预。

11） **主备集群高可用：**支持集群间的高可用模式；支持主备集群数据全量、增量同步；支持主备集群同步回滚机制；支持主备同步错误恢复机制； 支持同城灾备；

12） **安全性：**提供完善的用户、角色、权限控制策略，提高数据库集群的 安全性；支持详尽的审计日志，可配置灵活的审计策略，记录数据库 中与数据库

操作相关的所有日志，也可以通过图形化的监视工具实现 审计管理；支持透明的数据加密：支持数据存储加密，支持数据库密 码加密，支持数据加密压缩；支持相关加密函数，如 AES_ENCRYPT()、 ENCRYPT()、MD5()、SHA1()、SHA()等；支持库内数据脱敏；支持 Kerberos 认证方式访问集群和外部数据源；

13）易维护：提供图形化管理及监控工具，以简化管理员对数据库的管理 工作；

14） 数据加载高效性：基于策略的数据加载模式，集群整体加载速度大于 30TB/h；

15）数据备份恢复能力：支持实例级、库级、表级的全量、增量备份/恢 复；

16）Hadoop 备份/恢复：支持与 Hadoop 之间进行数据备份/恢复，将库内数据备份到 Hadoop 中，或将 Hadoop 内的数据文件恢复到库内；Hadoop 备份/恢复性能大于 100TB/小时；

17）标准化：支持 SQL 2003 ANSI/ISO 标准，支持 ODBC、JDBC、ADO.NET 等接口规范；支持 C API，Python API，TCL API 等接口；支持 OLAP 函数。

3.2.3.8 **大数据建设方案**

计算机科学领域的数据处理技术的发展，主要分为四个阶段：

阶段一：数据库时代。数据库最早诞生于 20 世纪的 60 年代，今天人们所熟知的关系型数据库则出现在 20 世纪 70 年代，并在后续的 30 年左右时间里大放异彩，诞生了很多优秀的关系型数据库，成为主流计算机系统不可或缺的组成部分。

阶段二：大数据技术的「探索期」。随着互联网的爆发，动辄几十亿、上百亿的页面以及海量的用户点击行为，开启了全球的数据量急剧增加的新时代。传统的数据库方案再也无力以可接受的成本提供计算力，巨大的数据处理需求开始寻找突破口，大数据时代开始萌芽。

阶段三：大数据技术的「发展期」。随着越来越多的资源投入到大数据计算领域，大数据技术进入一个蓬勃发展的阶段，整体开始从能用转向好用。代替昂贵的手写 MapReduce 作业的，则是出现各种以 SQL 为表达的计算引擎。这些计算引擎针对不同的场景进行针对性优化，但都采用门槛极低的 SQL 语言，极大降低了大数据技术的使用成本。

公共资源交易平台投标专用

阶段四：大数据技术「普及期」。当前，大数据技术已经渗透到各行各业，大数据的普及期已经到来。市场对大数据产品的要求，除了规模、性能、简单易用，提出了成本、安全、稳定性等更加全面的企业级生产的要求。

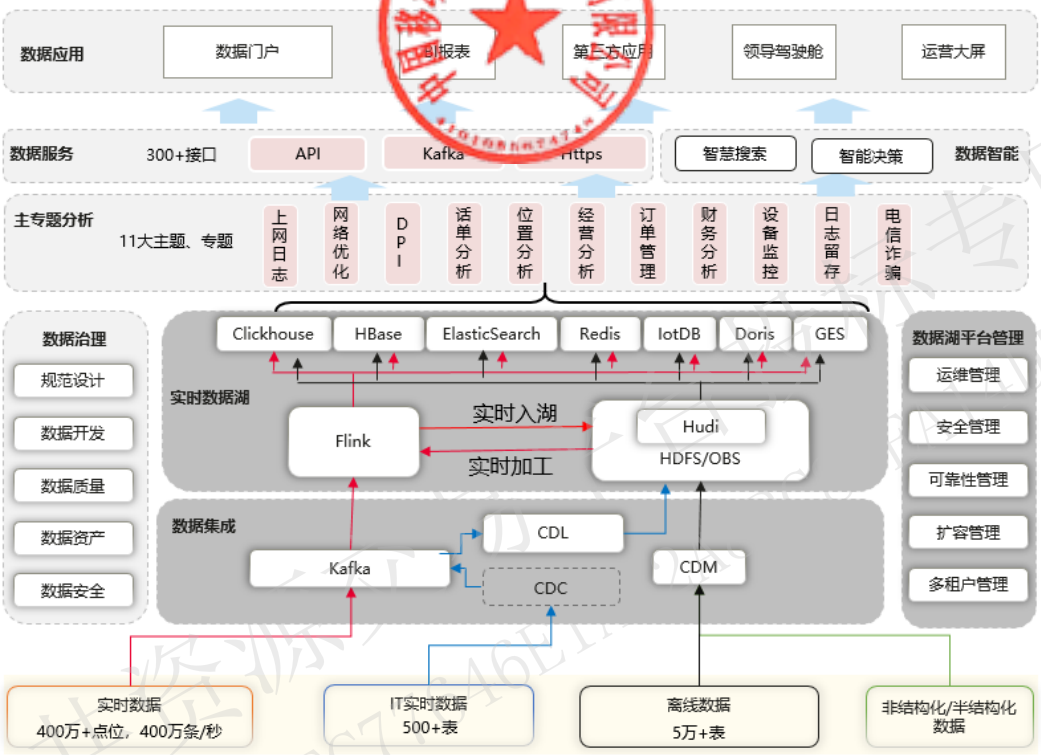
最开始的时候，每个应用程序会产生、存储大量数据，而这些数据并不能被其他应用程序使用，这种状况导致数据孤岛的产生。随后数据集市应运而生，应用程序产生的数据存储在一个集中式的数据仓库中，可根据需要导出相关数据传输给企业内需要该数据的部门或个人。然而数据集市只解决了部分问题。剩余问题，包括数据管理、数据所有权与访问控制等都亟须解决，因为企业寻求获得更高的使用有效数据的能力。为了解决前面提及的各种问题，企业有很强烈的诉求搭建自己的数据湖，数据湖不但能存储传统类型数据，也能存储任意其他类型数据，并且能在它们之上做进一步的处理与分析，产生最终输出供各类程序消费。

本次项目将建设数据湖作为企业内的数据基座。企业内的全量数据，包括实时数据、离线数据、半结构化/非结构化数据等，可以以实时或者批量的方式加载到数据湖中。数据在数据湖湖中进行统一存储和加工，并进行数据治理和主题建模。再根据业务需求将数据加载进不同的数据集市中，通过数据服务的统一接口服务对外开放数据。数据加载分为实时数据的加载和离线数据的加载。OT 类实时数据通过消息管道统一收集，IT 类实时数据需要配套数据库厂家提的 CDC 工具进行收集，收集后送入消息管道中。IT 实时数据入湖可以通过实时入湖工具进行数据同步入湖，OT 类数据可以使用实时流处理引擎进行数据的实时入湖。离线数据，包括离线 IT 数据和半结构化/非结构化文件数据，使用批量数据加载工具将数据加载到数据湖中。数据湖采用分布式统一存储组件进行各种类型数据的统一存储，并对结构化数据支持 ACID 操作，满足在数据湖内建仓建模的需求。数据湖存储采用开放存储格式，可以对接多种主流数据加工引擎，可以在数据湖之上利用多种计算引擎对数据进行处理，如 Hive、Spark、HetuEngine 等，且可以扩展对接数据挖掘和深度学习工具对数据湖之上的数据进行 AI 处理。

数据湖适用于数据的统一加工和治理，数据湖加工后的数据可以根据业务性能要求和查询模式要求将数据导入数据集市组件。数据集市组件可以在特定查询场景下提供极致的查询性能，可以更好的满足业务端数据快速呈现的需求。数据湖中的数据是共享的，全局唯一的。数据集市中的数据不同业务按需从数据湖中

加载，通常是非共享的，不同业务的数据可能是重复的。数据湖平台中提供的数据集市组件包括：实时 OLAP 分析引擎、实时精确检索数据库，实时综合搜索数据库、内存数据库、时序数据库等。

3.2.3.8.1 系统架构



数据湖从各种数据源，以批量和实时的方式将全量业务数据汇聚到数据湖平台中存储。并利用数据湖内丰富的计算引擎对数据进行加工，根据业务需要形成面向业务的专题集市。数据湖需要具有批流一体的数据加工能力，加快湖内数据的流转，更快的呈现数据价值，同时也完全支持传统批量加工业务。现在数据湖的特点体现在以下几个方面：

1. 数据入湖：通过批量集成、批量导入等工具，以定时加载或实时处理的方式，将常见的数据源（如业务数据库、FTP 文件系统、消息日志、IoT 设备等）的数据，批量接入到数据湖中进行批量加工分析。同时支持数据以实时追加或更新的方式进行入湖，利用批流一体的计算引擎进行数据的实时加工。

2. 数据存储：分布式存储系统，可线性扩展，支持结构化、半结构化、非结构化等各种形式数据存储。支持实时数据存储，支持 ACID 模式，支持存量数据的实时数据更新和删除。

3. 批流一体数据加工：支持批流一体数据加工模式，数据端到端加工延迟可以低至分钟级别。支持分布式计算架构，丰富的计算引擎支持，按照业务场景，支撑海量业务数据的实时和批量 ETL（抽取 Extract，转换 Transform,加载 Load）、逻辑程序处理、灵活查询等等多个场景所需的数据加工引擎。支持数据湖内的实时数据仓建设，采用批流一体加工引擎，结合 ACID 加工模式，及交互式查询引擎，数据入湖、加工、查询，分钟级完成端到端数据加工，并可以对加工结果进行即席查询。

4. 多样性数据集市：提供多种集市系统，满足不同业务系统的高效用数据需求。集市类型包含键值查询、全文检索、内存缓存、宽表查询、实时 OLAP、时序数据处理、图数据处理等。集市类型可灵活组合，按需使用。

3.2.3.8.2 服务能力

1、数据集成

数据源：数据源的种类包括流式数据（Socket 流，OGG 日志流、日志文件）、数据库、结构化/半结构化文件数据等。

实时消息管道：用于接收实时采集流式数据。通常在消息管道需要实时采集系统进行实时数据的采集，常见的有 Iot 数据采集工具、Flume、第三方 CDC 工具等。

实时入湖工具：用于 IT 数据的实时同步，可将 IT 数据库中发生的数据变更实时同步到数据湖中。

批量采集工具：用于批量采集数据库数据、数据文件、日志文件等数据，常见的有华为 DataArts Studio CDM、第三方 ETL 工具等。

2、数据存储

分布式文件系统：为各种批处理引擎提供数据存储，可以存储各种文件格式数据，常见格式有 Parquet 和 ORC 格式。

数据湖存储：提供分布式文件系统之上的 ACID 能力，可以支持历史数据的

公共资源交易平台技术专用
AE2C19C4C776E4CE1A62A8BC88EA14DB9

高效更新、增量查询等能力。

3、数据加工

统一资源调度引擎：为各种批处理引擎提供资源调度能力，是多租户资源分配的基础。

交互查询引擎：分布式交互查询引擎，用于实现高性能的交互式查询。适用于在海量数据快速查询少量结果数据的场景，如数据湖内的数据探索，湖内数据开放等。

实时流处理引擎：接收消息管道中的实时数据并进行处理，然后以批量的方式加载到数据湖中或者实时写入数据集市组件。支持批流一体加工模式，可直接对实时数据湖中的数据进行加工。

批处理引擎：用于实现高性能的离线批处理作业运行。

- **Hive**：传统 SQL 批处理引擎，用于处理 SQL 类批处理作业，使用广泛，海量数据下表现稳定，但是处理速度较慢；
- **MapReduce**：传统批处理引擎，用于处理非 SQL 类，尤其是数据挖掘和机器学习类批处理作业， 使用广泛，海量数据下表现稳定，但是处理速度较慢；
- **Tez**：基于 Mapreduce 改进的批处理引擎，在继承 MapReduce 稳定可靠的特点下，提供更高效的数据分析方式；
- **Spark SQL**：新型 SQL 批处理引擎，用于处理 SQL 类批处理作业，适合海量数据，处理速度高效；
- **Spark**：新型批处理引擎，用于处理非 SQL 类，尤其是数据挖掘和机器学习类批处理作业，适合海量数据，处理速度高效；

4、多样性集市

宽表分析引擎：适用于结构化数据单表聚合查询场景，可针对大宽表提供高效查询多维分析能力。

实时精确查询引擎：提供基于主键的全局排序存储模式，提供基于主键的高并发低延迟查询能力。

实时综合搜索引擎：可以对存储在其上的数据的任意资源创建高效索引，适用于全文检索和多字段综合搜索场景。

内存数据库：提供超高并发、超低延迟的 KV 检索查询能力。

时序数据库：针对时序数据的高效存储和分析数据库组件。

公共资源交易平台技标专用

实时 OLAP 引擎：提供结构化数据的综合实时分析能力，可支持高效的多表关联查询。

5、数据智能

实时决策引擎：通过预制的研判规则对实时流式数据进行实时研判分析，适用于决策分析、反欺诈等场景。

智慧搜索场景：通过内置的高效搜索引擎和用户友好的搜索界面为企业提供综合性的知识搜索查询能力。

6、数据湖平台管理

运维管理：各组件状态监控、启停、配置修改、日志查看等。

安全管理：对平台组件和数据访问提供统一的安全管控机制，保障数据湖平台数据安全。

可靠性管理：组件 HA 管理，容灾、备份管理，保障数据湖平台提供稳定可靠的服务。

扩容管理：可在线添加扩展新服务，及为已有服务扩容节点。

多租户管理：为不同租户分配不同资源和权限，实现资源的共享和隔离。

3.2.3.8.3 实时计算服务

实时数据湖是在数据从数据源产生后，可以实时进入到数据湖存储，数据时效性通常在 1 到 15 分钟之间。实时数据湖既可以用来支撑企业内部 T+1 小时级别的离线分析和处理，也可以支撑企业内部实时分析和处理。

实时数据湖注重数据的在湖内加工处理的时效性，在满足企业离线加工业务的前提下，还可以支持准实时的数据加工业务，一般包括如下大数据组件：Spark 分布式内存计算引擎、Hive 批量查询分析、HetuEngine 湖内交互式查询引擎、HDFS 分布式文件系统、Yarn 统一资源管理调度系统、Hudi ACID 加工、FlinkSQL 批流一计算引擎、Kafka 实时消息管道、实时入湖、批量入湖等组件。

实时数据湖可以提供分钟级延迟的数据入湖加工能力，可满足准实时业务的需求。作为实时数据湖的补充，实时数据也可以直接通过流处理系统加工后直接送入到数据集市组件中，供前端业务开展实时应用。此时数据不经过数据湖的统一加工处理过程，数据延迟可以低至毫米级，适用于需要访问原始数据，延迟要求苛刻的实时业务场景。

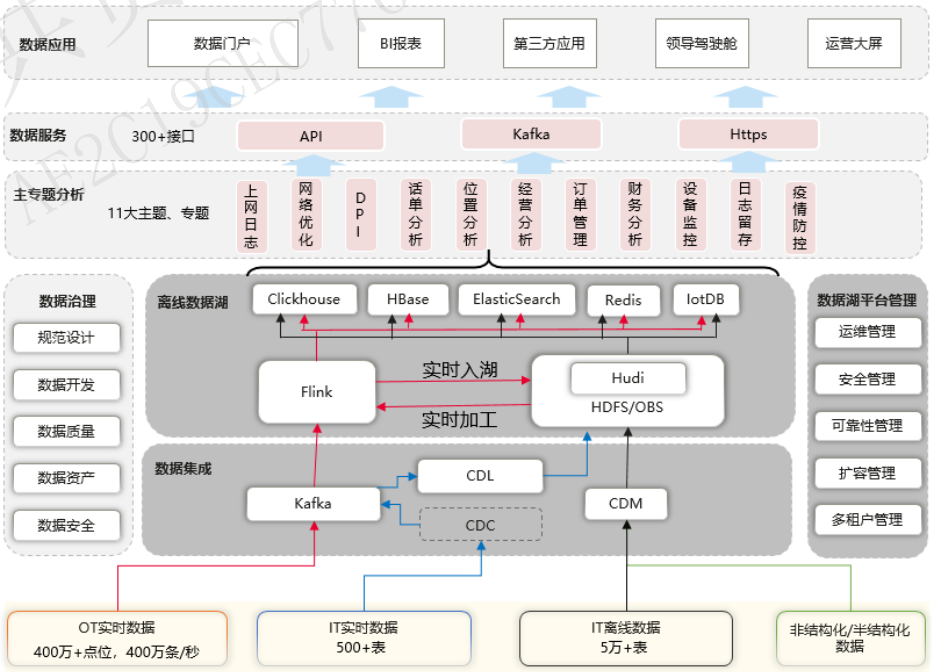
公共资源交易平台技术专用

实时数据湖从各种数据源，以批量和实时的方式将全量业务数据汇聚到数据湖平台中存储。并利用数据湖内丰富的计算引擎对数据进行加工，根据业务需要形成面向业务的专题集市。实时数据湖需要具有数据准实时加工的能力，加快湖内数据的流转，更快的呈现数据价值，同时也完全支持传统批量加工业务。实时数据湖的特点体现在以下几个方面：

1、实时数据入湖：支持数据以实时追加或更新的方式进行入湖，同时支持以批量加载的方式高效加载存量数据。

2、实时数据存储：分布式存储系统，存储模式支持实时数据存储，支持 ACID 模式，支持存量数据的实时数据更新和删除。可线性扩展，支持结构化、半结构化、非结构化等各种形式数据存储。

3、批流一体数据加工：支持批流一体数据加工模式，数据端到端加工延迟可以低至分钟级别。支持分布式计算架构，丰富的计算引擎支持，按照业务场景，支撑海量业务数据的实时和批量 ETL（抽取 Extract，转换 Transform，加载 Load）、逻辑程序处理、灵活查询等等多个场景所需的数据加工引擎。支持数据湖内的实时数据仓建设，采用批流一体加工引擎，结合 ACID 加工模式，及交互式查询引擎，数据入湖、加工、查询，分钟级完成端到端数据加工，并可以对加工结果进行即席查询。



本次项目将建设实时数据湖作为企业内的数据基座。企业内的全量数据，包括实时数据、离线数据、半结构化/非结构化数据等，可以以实时或者批量的方式加载到数据湖中。数据在数据湖湖中进行统一存储和加工，并进行数据治理和主题建模。再根据业务需求将数据加载进不同的数据集市中，通过数据服务的统一接口服务对外开放数据。数据加载分为实时数据的加载和离线数据的加载。OT 类实时数据通过消息管道统一收集，IT 类实时数据需要配套数据库厂家提的 CDC 工具进行收集，收集后送入消息管道中。IT 实时数据入湖可以通过实时入湖工具进行数据同步入湖，OT 类数据可以使用实时流处理引擎进行数据的实时入湖。离线数据，包括离线 IT 数据和半结构化/非结构化文件数据，使用批量数据加载工具将数据加载到数据湖中。数据湖采用分布式统一存储组件进行各种类型数据的统一存储，并对结构化数据支持 ACID 操作，满足在数据湖内建仓建模的需求。数据湖存储采用开放存储格式，可以对接多种主流数据加工引擎，可以在数据湖之上利用多种计算引擎对数据进行处理，如 Hive、Spark、HetuEngine 等，且可以扩展对接数据挖掘和深度学习工具对数据湖之上的数据进行 AI 处理。数据湖适用于数据的统一加工和治理，数据湖加工后的数据可以根据业务性能要求和查询模式要求将数据导入数据集市组件。数据集市组件可以在特定查询场景下提供极致的查询性能，可以更好的满足业务端数据快速呈现的需求。数据湖中的数据是共享的，全局唯一的。数据集市中的数据不同业务按需从数据湖中加载，通常是非共享的，不同业务的数据可能是重复的。数据湖平台中提供的数据集市组件包括：实时 OLAP 分析引擎、实时精确检索数据库，实时综合搜索数据库、内存数据库、时序数据库等。

实时数据湖可以提供分钟级延迟的数据入湖加工能力，可满足准实时业务的需求。作为实时数据湖的补充，实时数据也可以直接通过流处理系统加工后直接送入到数据集市组件中，供前端业务开展实时应用。此时数据不经过数据湖的统一加工处理过程，数据延迟可以低至毫米级，适用于需要访问原始数据，延迟要求苛刻的实时业务场景。

数据湖平台作为企业内的数据基座，除了提供核心的存储能力，还需要具备完善的管理运维能力。本次建设的离线数据湖平台提供统一的前端可视化管理界

面，可以对数据湖平台进行统一运维管理操作。数据湖平台提供完善的安全管控能力，保障数据湖的内数据安全可靠。本次建设的数据湖采用分布式部署架构，不存在单点故障，任意节点的故障不影响整体平台功能可用性。数据湖平台具备良好的扩展能力，可在线线性扩容，可满足业务长期增长的需求。最后，数据湖平台提供完整的多租户管理能力，企业内的多个业务系统可在数据湖之上进行资源共享、权限隔离，在保证数据安全的前提下，实现数据湖资源的充分利用。具体功能模块如下：

1、数据集成

数据源：数据源的种类包括流式数据（Socket 流，OGG 日志流、日志文件）、数据库、结构化/半结构化文件数据等。

实时消息管道：用于接收实时采集流式数据。通常在消息管道需要实时采集系统进行实时数据的采集，常见的有 Iot 数据采集工具、Flume、第三方 CDC 工具等。

实时入湖工具：用于 IT 数据的实时同步，可将 IT 数据库中发生的数据变更实时同步到数据湖中。

批量采集工具：用于批量采集数据库数据、数据文件、日志文件等数据，常见的有华为 DataArts Studio CDM、第三方 ETL 工具等。

2、数据存储

分布式文件系统：为各种批处理引擎提供数据存储，可以存储各种文件格式数据，常见格式有 Parquet 和 ORC 格式。

数据湖存储：提供分布式文件系统之上的 ACID 能力，可以支持历史数据的高效更新、增量查询等能力。

3、数据加工

统一资源调度引擎：为各种批处理引擎提供资源调度能力，是多租户资源分配的基础。

交互查询引擎：分布式交互查询引擎，用于实现高性能的交互式查询。适用于在海量数据快速查询少量结果数据的场景，如数据湖内的数据探索，湖内数据开放等。

实时流处理引擎：接收消息管道中的实时数据并进行处理，然后以批量的方式加载到数据湖中或者实时写入数据集市组件。支持批流一体加工模式，可直接对实时数据湖中的数据进行加工。

批处理引擎：用于实现高性能的离线批处理作业运行。

Hive：传统 SQL 批处理引擎，用于处理 SQL 类批处理作业，使用广泛，海量数据下表现稳定，但是处理速度较慢；

MapReduce：传统批处理引擎，用于处理非 SQL 类，尤其是数据挖掘和机器学习类批处理作业， 使用广泛，海量数据下表现稳定，但是处理速度较慢；

Tez：基于 Mapreduce 改进的批处理引擎，在继承 MapReduce 稳定可靠的特点下，提供更高效的数据分析方式；

Spark SQL：新型 SQL 批处理引擎，用于处理 SQL 类批处理作业，适合海量数据，处理速度高效；

Spark：新型批处理引擎，用于处理非 SQL 类，尤其是数据挖掘和机器学习类批处理作业，适合海量数据，处理速度高效；

4、数据集市

实时 OLAP 引擎：适用于结构化数据单表聚合查询场景，可针对大宽表提供高效查询多维分析能力。

实时精确查询引擎：提供基于主键的全局排序存储模式，提供基于主键的高并发低延迟查询能力。

实时综合搜索引擎：可以对存储在其上的数据的任意资源创建高效索引，适用于全文检索和多字段综合搜索场景。

内存数据湖：提供超高并发、超低延迟的 KV 检索查询能力。

时序数据库：针对时序数据的高效存储和分析数据库组件。

5、数据湖平台管理

运维管理：各组件状态监控、启停、配置修改、日志查看等。

安全管理：对平台组件和数据访问提供统一的安全管控机制，保障数据湖平台数据安全。

可靠性管理：组件 HA 管理，容灾、备份管理，保障数据湖平台提供稳定可靠的服务。

公共资源交易平台投标专用

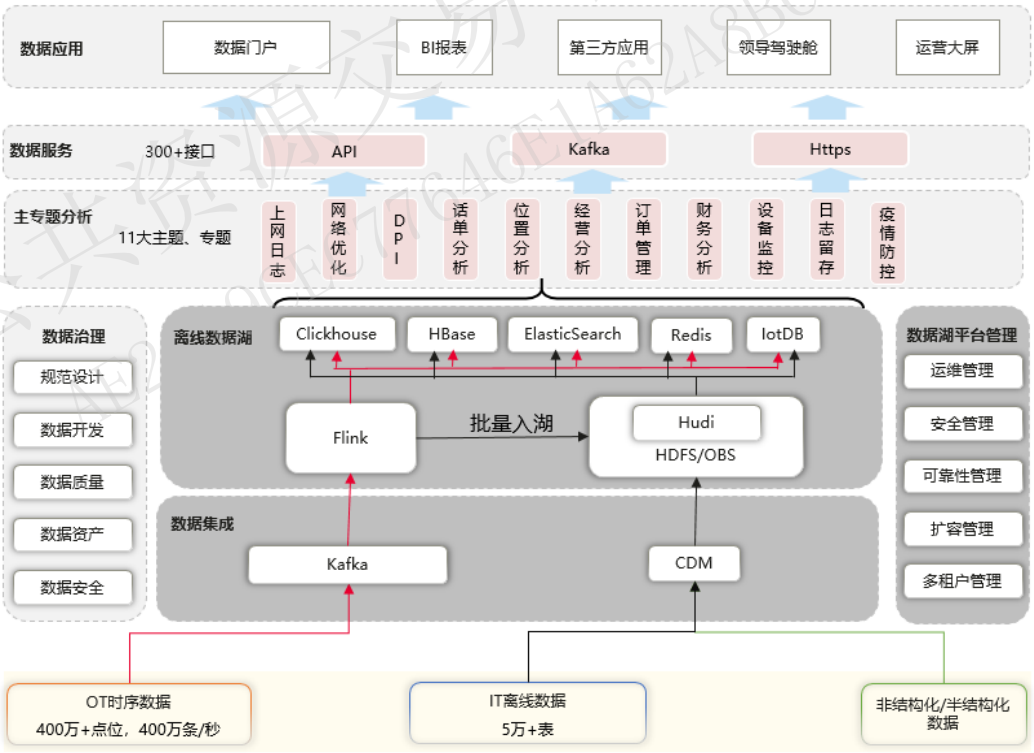
扩容管理：可在线添加扩展新服务，及为已有服务扩容节点。

多租户管理：为不同租户分配不同资源和权限，实现资源的共享和隔离。

3.2.3.8.4 离线计算服务

离线数据湖是针对数据时效性要求不高的场景，将多种格式的数据源汇聚到大数据平台，通过严格的数据权限和资源管控，将数据和算力开放给各种使用者。数据从数据源的产生，到入湖存储，无需做到实时供数，数据的时效性要求通常在 15 分钟以上。

离线数据湖主要用来支撑企业内部 T+1 的离线分析和处理工作，一般包括如下大数据组件：Spark 分布式内存计算引擎、Hive 批量查询分析、HetuEngine 湖内交互式查询引擎、HDFS 分布式文件系统、Yarn 统一资源管理调度系统、Hudi ACID 加工、批量入湖等组件；另外，在离线数据湖中，实时流处理能力可以作为独立的实时流处理单元，独立完成实时数据处理，并将处理结果直接加载到数据集市或者批量加载到数据湖中，一般包括组件：Kafka 实时消息管道、Flink 实时流处理组件。



本次项目将建设离线数据湖作为企业内的数据基座。企业内的全量数据，包括实时数据、离线数据、半结构化/非结构化数据等，可以以批量的方式加载到

数据湖中。数据在数据湖中进行统一存储和加工，并进行数据治理和主题建模。再根据业务需求将数据加载进不同的数据集市中，通过数据服务的统一接口服务对外开放数据。数据加载分为实时数据的加载和离线数据的加载，实时数据通过消息管道统一收集，并使用流处理引擎每隔一段时间将数据加载进数据湖统一存储中。离线数据使用批量数据加载工具将数据加载到数据湖中。数据湖采用分布式统一存储组件进行各种类型数据的统一存储，并对结构化数据支持 ACID 操作，满足在数据湖内建仓建模的需求。数据湖存储采用开放存储格式，可以对接多种主流数据加工引擎，可以在数据湖之上利用多种计算引擎对数据进行处理，如 Hive、Spark、HetuEngine 等，且可以扩展对接数据挖掘和深度学习工具对数据湖之上的数据进行 AI 处理。数据湖适用于数据的统一加工和治理，数据湖加工后的数据可以根据业务性能要求和查询模式要求将数据导入数据集市组件。数据集市组件可以在特定查询场景下提供极致的查询性能，可以更好的满足业务端数据快速呈现的需求。数据湖中的数据是共享的，全局唯一的。数据集市中的数据不同业务按需从数据湖中加载，通常是非共享的，不同业务的数据可能是重复的。数据湖平台中提供的数据集市组件包括：实时 OLAP 分析引擎、实时精确检索数据库，实时综合搜索数据库、内存数据库、时序数据库等。

作为离线数据湖的补充，实时数据也可以直接通过流处理系统加工后直接送入到数据集市组件中，供前端业务开展实时应用。此时数据不经过数据湖的统一加工处理过程，数据延迟可以低至毫米级，适用于需要访问原始数据，延迟要求苛刻的实时业务场景。

数据湖平台作为企业内的数据基座，除了提供核心的存储能力，还需要具备完善的管理运维能力。本次建设的离线数据湖平台提供统一的前端可视化管理界面，可以对数据湖平台进行统一运维管理操作。数据湖平台提供完善的安全管控能力，保障数据湖的内数据安全可靠。本次建设的数据湖采用分布式部署架构，不存在单点故障，任意节点的故障不影响整体平台功能可用性。数据湖平台具备良好的扩展能力，可在线线性扩容，可满足业务长期增长的需求。最后，数据湖平台提供完整的多租户管理能力，企业内的多个业务系统可在数据湖之上进行资源共享、权限隔离，在保证数据安全的前提下，实现数据湖资源的充分利用。具体功能模块如下：

1、数据集成

数据源：数据源的种类包括流式数据（Socket 流，OGG 日志流、日志文件）、数据库、结构化/半结构化文件数据等。

实时消息管道：用于接收实时采集流式数据。消息管道通常需要配合实时采集系统进行实时数据的采集，常见的有 Iot 数据采集工具、Flume、第三方 CDC 工具等。

批量采集工具：用于批量采集数据库数据、数据文件、日志文件等数据，常见的有华为 DataArts Studio CDM、第三方 ETL 工具等。

2、数据存储

分布式文件系统：为各种批处理引擎提供数据存储，可以存储各种文件格式数据，常见格式有 Parquet 和 ORC 格式的格式。

数据湖存储：提供分布式文件系统之上的 ACID 能力，可以支持历史数据的高效更新、增量查询等能力。

3、数据加工

统一资源调度引擎：为各种批处理引擎提供资源调度能力，是多租户资源分配的基础。

交互查询引擎：分布式交互查询引擎，用于实现高性能的交互式查询。适用于在海量数据快速查询少量结果数据的场景，如数据湖内的数据探索，湖内数据开放等。

实时流处理引擎：接收消息管道中的实时数据并进行处理，然后以批量的方式加载到数据湖中或者实时写入数据集市组件。

批处理引擎：用于实现高性能的离线批处理作业运行。

Hive：传统 SQL 批处理引擎，用于处理 SQL 类批处理作业，使用广泛，海量数据下表现稳定，但是处理速度较慢；

MapReduce：传统批处理引擎，用于处理非 SQL 类，尤其是数据挖掘和机器学习类批处理作业， 使用广泛，海量数据下表现稳定，但是处理速度较慢；

Tez：基于 Mapreduce 改进的批处理引擎，在继承 MapReduce 稳定可靠的特点下，提供更高效的数据分析方式；

公共资源交易平台投标专用

Spark SQL：新型 SQL 批处理引擎，用于处理 SQL 类批处理作业，适合海量数据，处理速度高效；

Spark：新型批处理引擎，用于处理非 SQL 类，尤其是数据挖掘和机器学习类批处理作业，适合海量数据，处理速度高效；

4、数据集市

实时 OLAP 引擎：适用于结构化数据单表聚合查询场景，可针对大宽表提供高效查询多维分析能力。

实时精确查询引擎：提供基于主键的全局排序存储模式，提供基于主键的高并发低延迟查询能力。

实时综合搜索引擎：可以对存储在其上的数据的任意资源创建高效索引，适用于全文检索和多字段综合搜索场景。

内存数据湖：提供超高并发、超低延迟的 KV 检索查询能力。

时序数据库：针对时序数据的高效存储和分析数据库组件。

5、数据湖平台管理

运维管理：各组件状态监控、启停、配置修改、日志查看等。

安全管理：对平台组件和数据访问提供统一的安全管控机制，保障数据湖平台数据安全。

可靠性管理：组件 HA 管理，容灾、备份管理，保障数据湖平台提供稳定可靠的服务。

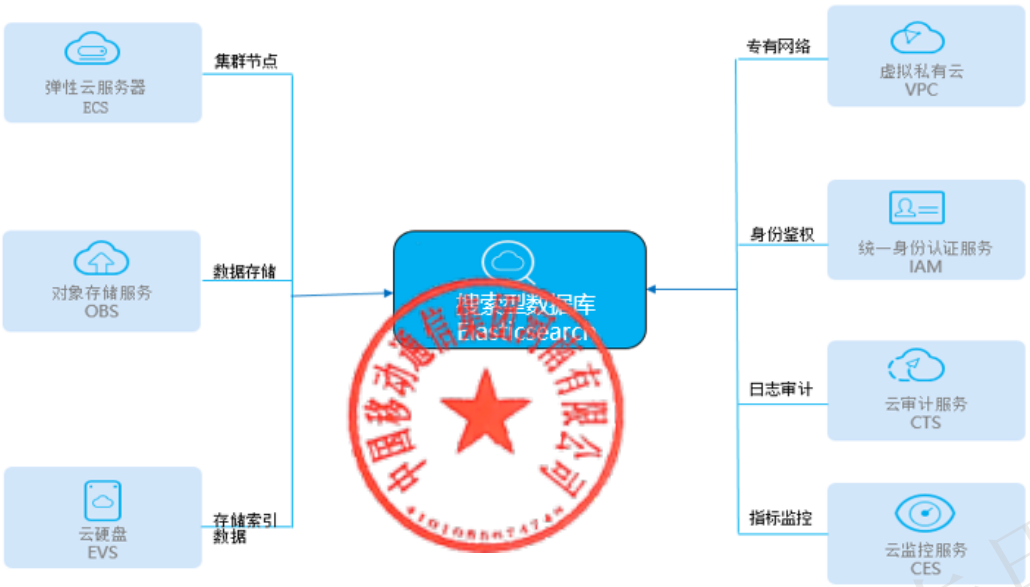
扩容管理：可在线添加扩展新服务，及为已有服务扩容节点。

多租户管理：为不同租户分配不同资源和权限，实现资源的共享和隔离。

3.2.3.8.5 搜索引擎服务

搜索型数据库致力于信息检索、数据的多维查询和统计分析等场景。使用云平台提供的索型数据库，可以快速部署、轻松管理、按需扩展集群，简化复杂的运维操作，更加聚焦于业务本身。整体技术架构如下图所示：

公共资源交易平台投标专用



- 集群

云搜索服务是以集群为单位进行组织，一个集群代表一个独立运行的搜索服务，由多个节点构成。

- 索引

用于存储 Elasticsearch 的数据，是一个或多个分片分组在一起的逻辑空间。

- Shard

索引可以存储数据量超过 1 个节点硬件限制的数据。为满足这样的需求，Elasticsearch 提供了一个能力，将一个索引拆分为多个，称为 Shard。当您创建一个索引时，您可以根据实际情况指定 Shard 的数量。每个 Shard 托管在集群中的任意一个节点中，且每个 Shard 本身是一个独立的、全功能的“索引”。

Shard 的数量只能在创建索引前指定，且在索引创建成功后无法修改。

- Replica（副本）

Shard 下的实际存储索引的一个副本。可以理解为备份 Shard。副本的存在可以预防单节点故障。使用过程中，您可以根据业务情况增加或减少 Replica 数量。

- 文档

公共资源交易平台投标专用

Elasticsearch 存储的实体，是可以被索引的基本单位，相当于关系型数据库中的行。

- 文档类型

类似关系型数据库中的表，用于区分不同的数据。

Elasticsearch 7.x 以下版本中，1 个索引里面可以包含若干个文档类型，每个文档必须设定它的文档类型。

Elasticsearch 7.x 及以上版本，文档类型只支持“_doc”。

- 映射

用来约束字段的类型，可以根据数据自动创建。相当于数据库中的 Schema。

- 字段

组成文档的最小单位。相当于数据库中的 Column。

- 产品功能

兼容 Elasticsearch 原生接口

兼容开源 Elasticsearch 软件原生接口，完美支持 Beats、Kibana 等周边生态。

- 接入多种数据源

无缝对接 Ftp/Obs/Hbase/Kafka 等多种数据源，仅需简单配置，无需编程。

- 一键化操作

一键申请集群、一键扩容、一键重启，从小规模测试到大规模上线，所有主要操作都是一键可达。

- 灵活词库管理

支持自定义词库与拼音分词，支持词库热更新，无需重启，配置即生效。

- 自定义快照策略

公共资源交易平台投标专用
AE2C13CEC77646E1A62A8BC88EA14DB9

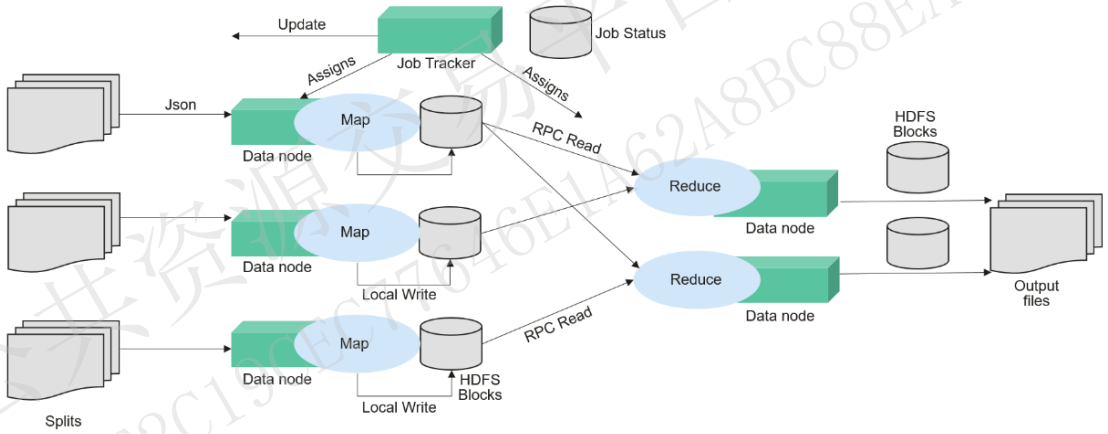
支持用户触发以及定时触发的快照备份能力，支持恢复到本集群以及其他集群的能力，随时恢复误删数据或者迁移数据到新的搜索集群。

3.2.3.8.6 分析计算服务

MapReduce 是 Hadoop 的核心，是 Google 提出的一个软件架构，用于大规模数据集（大于 1TB）的并行运算。概念“Map（映射）”和“Reduce（化简）”，及他们的主要思想，都是从函数式编程语言借来的，还有从矢量编程语言借来的特性。

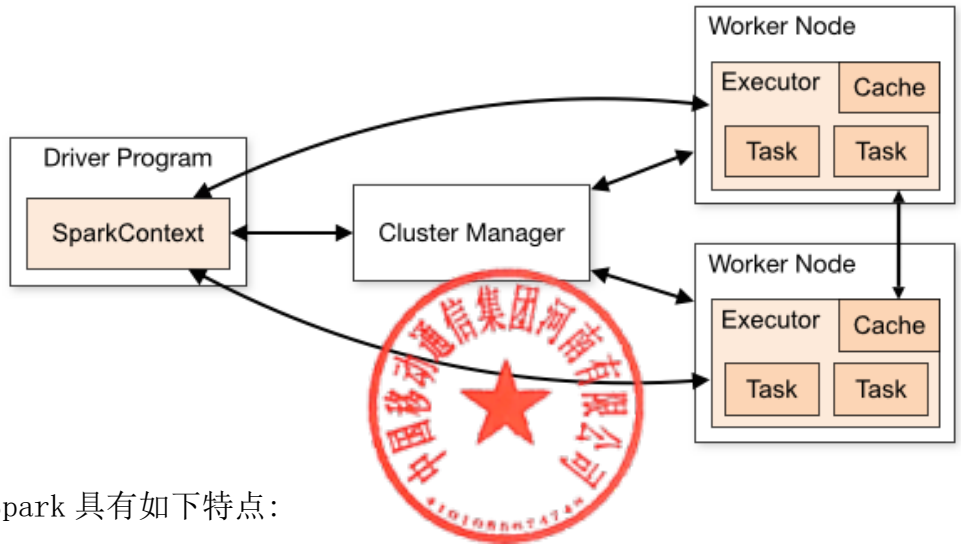
当前的软件实现是指定一个 Map（映射）函数，用来把一组键值对映射成一组新的键值对，指定并发的 Reduce（化简）函数，用来保证所有映射的键值对中的每一个共享相同的键组。

图1-1 分布式批处理引擎



MapReduce 是用于并行处理大数据集的软件框架。MapReduce 的根源是函数性编程中的 map 和 reduce 函数。Map 函数接受一组数据并将其转换为一个键/值对列表，输入域中的每个元素对应一个键/值对。Reduce 函数接受 Map 函数生成的列表，然后根据它们的键缩小键/值对列表。MapReduce 起到了将大事务分散到不同设备处理的能力，这样原本必须用单台较强服务器才能运行的任务，在分布式环境下也能完成了。

Apache Spark 是一个开源的，通用的分布式集群计算引擎。



Spark 具有如下特点:

快速：数据处理能力，比 MapReduce 快 10-100 倍。

易用：可以通过 Java，Scala，Python，简单快速的编写并行的应用处理大数据量，Spark 提供了超过 80 种高层的操作符来帮助用户组件并行程序。

普遍性：Spark 提供了众多高层的工具，例如 Spark SQL，MLib，GraphX，Spark Stream，可以在一个应用中，方便的将这些工具进行组合。

Spark 提供了一个快速的计算,写入,以及交互式查询的框架。相比于 Hadoop，Spark 拥有明显的性能优势。Spark 使用 in-memory 的计算方式，通过这种方式来避免一个 MapReduce 工作流中的多个任务对同一个数据集进行计算时的 IO 瓶颈。Spark 利用 Scala 语言实现，Scala 能够使得处理分布式数据集时，能够像处理本地化数据一样。

除了交互式的数据分析，Spark 还能够支持交互式的数据挖掘，由于 Spark 是基于内存的计算，很方便处理迭代计算，而数据挖掘的问题通常都是对同一份数据进行迭代计算。除此之外,Spark 能够运行于安装 Hadoop 2.0 Yarn 的集群。之所以 Spark 能够在保留 MapReduce 容错性，数据本地化，可扩展性等特性的同时，能够保证性能的高效，并且避免繁忙的磁盘 IO，主要原因是因为 Spark 创建了一种叫做 RDD（Resilient Distributed Dataset）的内存抽象结构。

原有的分布式内存抽象，例如 key-value store 以及数据库，支持对于可变状态的细粒度更新,这一点要求集群需要对数据或者日志的更新进行备份来保障容错性。这样就会给数据密集型的工作流带来大量的 IO 开销。而对于 RDD 来说，它只有一套受限制的接口，仅仅支持粗粒度的更新，例如 map，join 等等。通过这

种方式，Spark 只需要简单的记录建立数据的转换操作的日志，而不是完整的数据集，就能够提供容错性。这种数据的转换链记录就是数据集的溯源。由于并行程序，通常是对一个大数据集应用相同的计算过程，因此之前提到的粗粒度的更新限制并没有想象中的大。事实上，Spark 论文中阐述了 RDD 完全可以作为多种不同计算框架，例如 MapReduce，Pregel 等的编程模型。

并且，Spark 同时提供了操作允许用户显示的将数据转换过程持久化到硬盘。对于数据本地化，是通过允许用户能够基于每条记录的键值，控制数据分区实现的。（采用这种方式的一个明显好处是，能够保证两份需要进行关联的数据将会被同样的方式进行哈希）。如果内存的使用超过了物理限制，Spark 将会把这些比较大的分区写入到硬盘，由此来保证可扩展性。

3.2.3.9 **容器建设方案**

3.2.3.9.1 系统架构

容器是一种轻量级虚拟化技术，虚机启动可能需要数分钟或者更长，而容器只需数秒钟。传统虚拟技术是在硬件层面实现虚拟化，有性能损耗，而容器技术是以共享内核的方式实现，几乎无损耗。虚拟机更擅长于彻底隔离整个运行环境，而容器通常用于隔离不同的应用

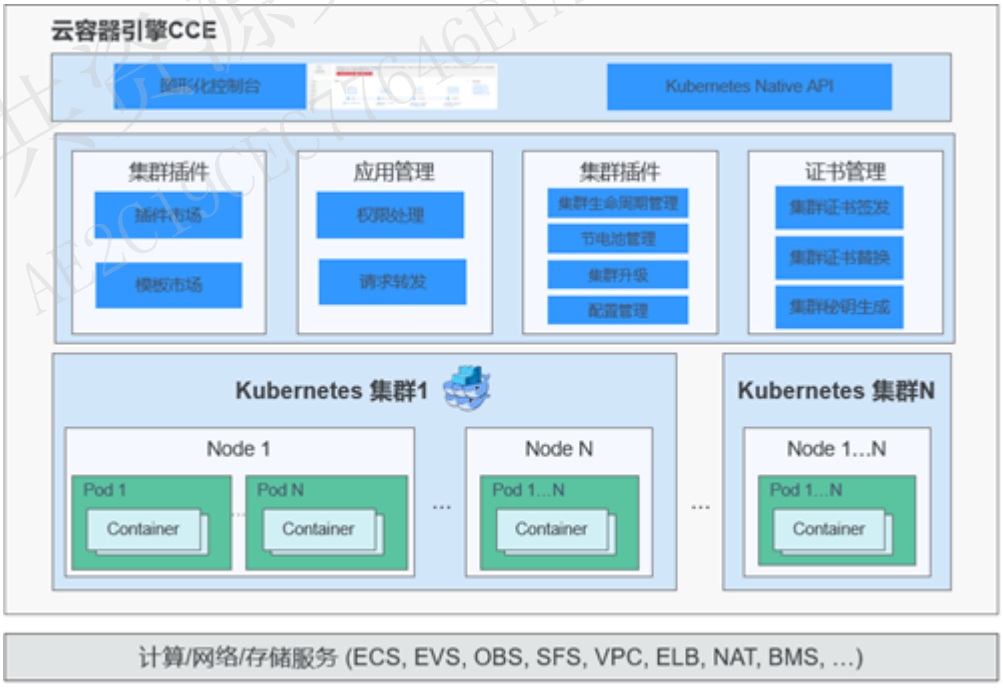


图 0-3 CCE系统架构

3.2.3.9.2 服务能力

功能点	功能点描述	备注
集群生命周期管理	支持集群的创建、休眠、唤醒、删除，支持Kubernetes 1.19	-
CCE集群	一键式创建CCE集群，集群内支持虚拟机与裸金属、x86和ARM、GPU、NPU等异构节点的混合部署	-
高性能集群调度器	自研高性能集群调度器Volcano	-
节点管理	支持节点动态纳管和静态纳管	
X86+G卡	支持X86+G芯片节点	支持Tesla P100、Tesla T4
A+D卡	支持鲲鹏+D芯片节点	支持D310
支持IPv6	数据面节点支持IPv4&v6双栈	
容器网络管理	支持overlay l2容器网络，支持L3 VPC Router容器网络	
容器存储管理	支持存储生命周期基本操作（创建、删除、挂载、卸载），支持EVS、SFS、OBS各类型存储	
工作负载管理	支持无状态、有状态、短任务、定时任务、守护进程部署，	
应用调度策略	亲和调度策略： 支持多个应用亲和调度到同一个节点。 支持应用亲和调度到指定标签的节点。 反亲和调度策略：	

公共资源交易平台投标专用

功能点	功能点描述	备注
	支持多个应用反亲和调度到不同节点。 支持应用反亲和调度到与指定标签不同的节点。	
弹性伸缩	1、提供基于原生策略、周期策略、告警策略的集群节点弹性伸缩能力 2、提供基于CPU/MEM策略，周期策略以及自定义指标策略的应用实例弹性伸缩能力	
应用升级	支持替换升级、滚动升级（按比例、实例个数 进行滚动升级）;升级回滚	
应用健康检查	提 供 liveness Probe 、readiness Probe两种探针的健康检查。	
应用配置管理	支持configmap和secret	
helm模板管理	提供Helm应用市场功能管理Helm模板，并可在Helm应用市场中直接管理通过Helm模板部署的应用	
插件管理	支 持 coredns 、 vaolcano 、everest、autoscaler等插件	
支持飞腾海光服务器	支持飞腾海光服务器	飞腾仅支持2000+
支持集群版本升级	支持集群版本从1.13升级到1.15	

CCE特性能力

公共资源交易平台投标专用

3.2.3.10 **应用建设方案**

3.2.3.10.1 应用托管与微服务治理

（一）系统架构

提供应用管理能力，并使用环境规划复杂的基础设施资源，通过运维管理能力统一运维应用与资源，支持多种主流微服务框架的服务治理，帮助企业打造100%在线、易管理、易运维、大规模的软件系统。



ROMA Factory系统架构

组件	说明
多种微服务兼容	兼容主流框架，并可打通微服务系统隔离，统一进行微服务治理。可使用服务网格接入与框架接入的微服务共同治理
应用管理	提供应用生命周期管理能力。
环境管理	基础设施的合集，可以统一规划基础设施。以环境为维度进行应用的部署管理。

ROMA Factory组件列表

ROMA Factory 吸收了华为全面云化转型的成功经验和技术创新成果，聚焦应用管理，对应用监控运维服务，容器镜像服务以及中间件服务进行了深度整合，全力打造功能齐全的一站式应用云平台。

- 支持双模微服务开发模式

同时支持传统的微服务框架开发方式以及服务网格接入方式将组件快速微服务化并进行统一治理运维，打通 spring cloud，服务网格与 ServiceComb 之间的隔离。以往用户只能选择服务网格或者传统开发框架之一来构建应用系统，

而现在 ROMA factory 为用户提供统一一致的体验，通过一致的微服务解决方案应对多变的业务需求。

- 基于契约进行微服务开发

支持一次编写代码，自动生成符合 Open API 2.0 标准的契约描述，可以保证微服务团队之间的高效合作。以契约为依据，加快生产效率。

- 开源兼容

兼容开源的 Java chassis，Spring Cloud，Dubbo，Go chassis 框架，帮助已经使用开源方案的用户无缝迁移到云平台。并为开源用户提供新特性。

- 微服务治理

通过容错，熔断，限流等技术手段提升业务系统韧性，提升业务稳定性。治理规则秒级下发。在系统承受攻击或异常流量时能够承受并保持在特定的运行状态，恢复并适应攻击以保证业务系统完成关键任务。

- 统一管理基础设施与多环境规划

以环境组织基础设施，简化基础设施的管理；选择环境部署应用，提高应用部署效率；以环境维度监控资源使用情况，提高资源的利用率，降低企业成本；由开发到测试到生产的多环境规划，规范应用从开发到上线的流程，加快业务上线。

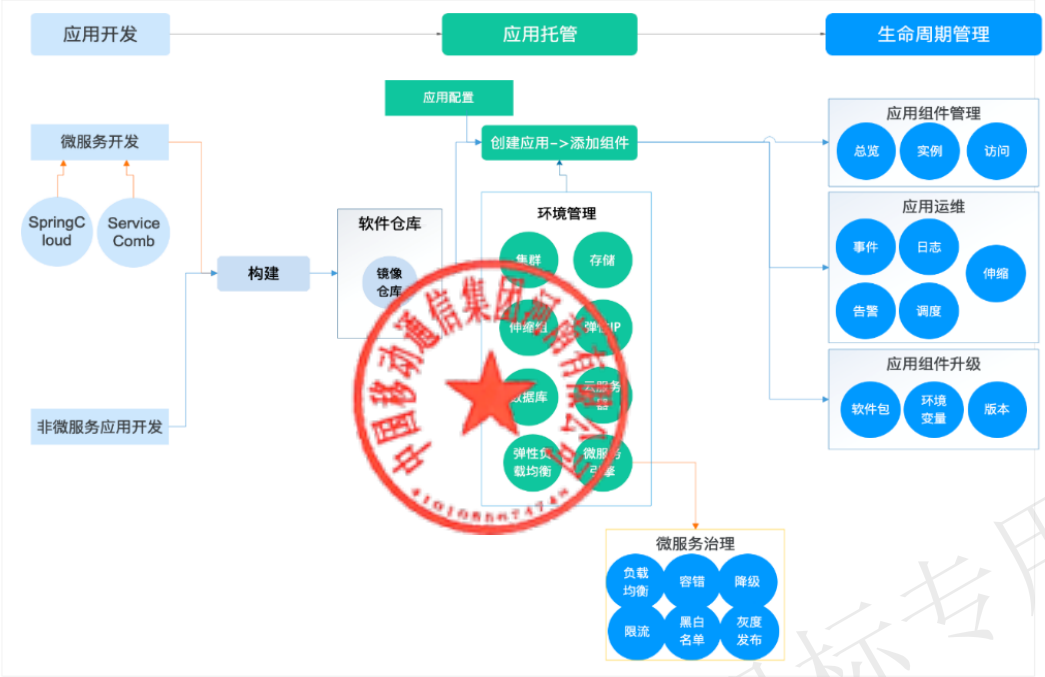
- 以应用为中心的全生命周期管理

规范应用、组件模型，以软件包定义应用组件，引导进行业务的解耦拆分，简化业务系统的复杂性；集成构建，流水线升级多个环境，进行应用组件的持续发布，提高上线效率；集成日志，监控指标，阈值告警等运维监控能力，提供升级回退、弹性伸缩、启停等运维操作。

(二)服务能力

提供应用托管、生命周期管理等功能，支持 Java、Go、Node.js、Docker、Tomcat、ServiceComb，Spring Cloud 等运行环境。

公共资源交易平台投标专用



应用管理功能架构

1.微服务引擎

提供微服务专享引擎，可以申请多个引擎，每个引擎具备注册发现，配置管理，微服务治理，认证鉴权等能力。

- 提供注册发现能力，包括OpenAPI文档管理，注册和发现能力，多种可视化指标。
- 提供配置管理能力，包括秒级配置推送，一键回滚，历史版本管理等特性。
- 认证鉴权，微服务接入注册发现，配置管理时需要提供身份信息进行认证。提升系统安全性 。
- 自动文档生成能力，只需要编写代码即可自动生成文档并注册到服务中心进行观察。
- 提供云上注册发现和配置管理能力，免运维。

2.Spring Cloud 接入

提供 Spring Cloud Huawei 接入微服务引擎，提供多种能力增强仅需修改配置，即可接入微服务引擎

3.多种微服务框架接入

公共资源交易平台投标专用

无论你还使用何种语言或者微服务开发框架，均可统一接入到微服务引擎当中。

4.微服务治理

接入到微服务引擎即可进行服务治理，支持的服务治理策略如下：

名称	说明
负载均衡	当出现访问量和流量较大，一台服务器无法负载的情况下，我们可以通过设置负载均衡的方式将流量分发到多个服务器均衡处理，从而降低时延，防止服务器过载。
限流	对服务实例设置限流，对当前服务实例的每秒请求数量超过设定的值时，当前服务实例就不再接受其他对象的调用请求。
重试	重试是服务实例出现异常时的一种处理策略，出现异常后按照定义的策略进行重试或访问新的服务实例。
降级	降级是容错的一种特殊形式，当出现服务吞吐量巨大，资源不够用等情况，可使用降级机制关掉部分不重要、性能较差的服务，避免占用资源，以保证主体业务功能可正常使用。
熔断	当由于某些原因导致服务出现了过载现象，为避免造成整个系统故障，可采用熔断来进行保护。
错误注入	错误注入策略用于测试微服务的容错能力，可以让用户知道，当出现延时或错误时，系统是否能够正常运行。

表 0-4 微服务治理策略

5.应用托管

应用可以托管在 Roma Factory 上。

- 支持从软件中心获取jar/war/zip/镜像，实现应用部署。
- 支持SpringCloud、Java Chassis等多种微服务框架托管。

公共资源交易平台投标专用

- 支持多种语言应用部署，支持微服务，Web服务多种服务类型。

支持托管的应用类型如下。

多应用组件类型	支持微服务、Web、通用
多微服务框架	支持Java chasis、SpringCloud、服务网格
多语言	支持Java、Go、NodeJs等主流开发语言
异构部署	支持CCE、虚机部署引擎
多部署来源格式	支持Jar、War、Zip、Docker Image

应用托管类型

6.环境管理

可以使用环境管理多种云服务基础设施，例如 CCE，ECS 等基础资源，VPC，EIP 等可选资源。

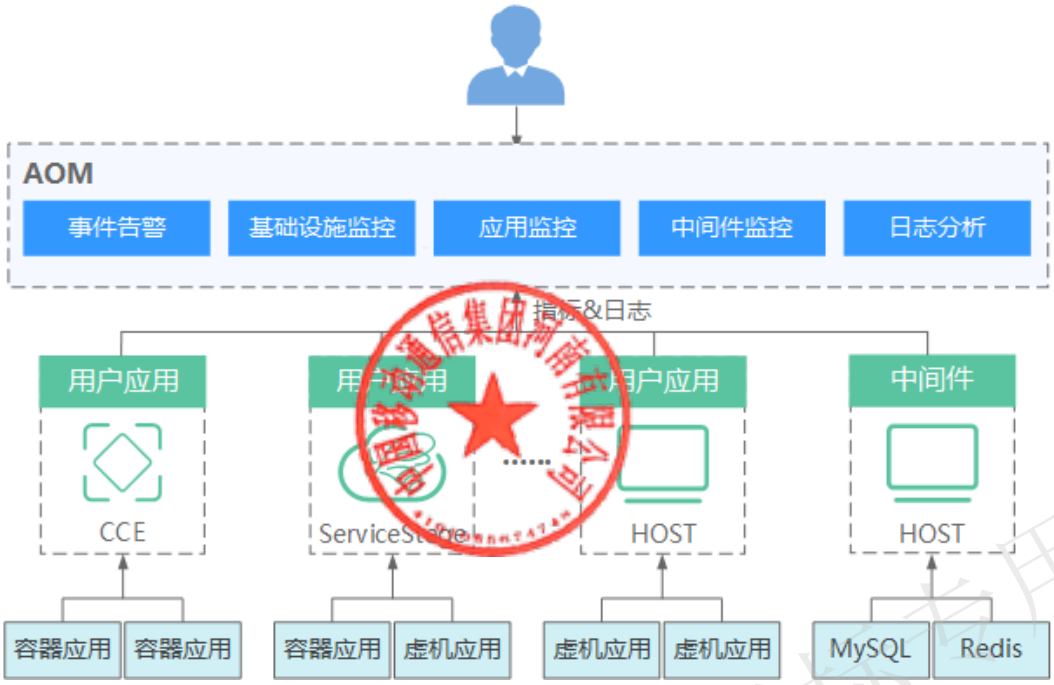
- 职责分离：应用开发与运维人员选择环境进行应用部署，简化应用部署的操作复杂度。环境管理员通过环境集中管理基础设施，提高资源利用率，降低成本。
- 持续发布：定义开发环境，测试环境，生产环境，通过流水线的连接，引导应用进行持续集成发布。

3.2.3.10.2 AOM 应用运维与日志管理

（一）系统架构

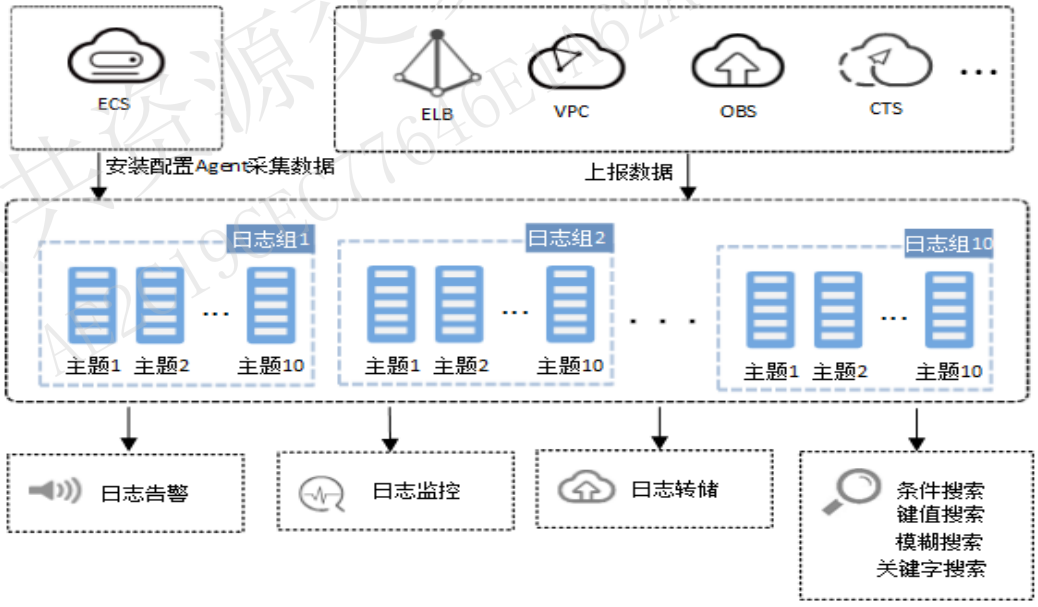
应用运维管理（Application Operations Management，简称 AOM）是云上应用的一站式立体化运维管理平台，实时监控用户的应用及相关云资源，采集并关联资源的各项指标、日志及事件等数据共同分析应用健康状态，提供灵活的告警及丰富的数据可视化功能，帮助用户及时发现故障，全面掌握应用、资源及业务的实时运行状况。

公共资源交易平台投标专用



AOM系统架构

云日志服务（Log Tank Service，简称 LTS）是一个可以进行日志收集、实时查询、转储等功能的服务；您无需开发即可利用日志服务做实时决策分析，提升日志处理效率。



LTS日志管理系统架构

云日志服务针对日志类数据提供预览与检索能力，提供秒级查找和定位问题的能力，帮助您提升运维、运营效率，轻松应对常见运维运营场景，如排查服务器障碍、应用程序 Bug 跟踪分析、业务数据分析等。

日志采集与转储：

- 弹性云服务器用户可以根据实际需求，安装并配置Agent，日志数据则会被采集到指定的日志组和日志流下。
- 云日志服务管理控制台会将采集到的日志保存1~30天，如需要长期保存，需要配置转储，云日志服务会将采集到的日志转储到用户定义的OBS桶中进行长期保存。

日志事件的查询与分析：

- 在“日志管理”页面，进入已创建的日志组和日志流下，您可以按照关键字等方式进行日志预览与全文搜索，来查看已采集的日志事件。
- 在“设置搜索”页面，可以创建快速查询、执行快速查询，查看日志数据的详细信息，并查看上下文。

（二）**服务能力**

功能点	功能点描述
监控总览	提供资源、应用等各种数据的集中监控、展示。 监控概览 提供了资源、应用、应用用户体验的全链路、多层次、一站式运维界面。 仪表盘 通过仪表盘可将不同图表展示到同一个屏幕上，通过曲线图、状态图、数字图等不同的仪表形式来展示资源数据，例全面、深入地掌握监控数据。用户可以创建自定义仪表盘，添加自己关注的指标图表到仪表盘，图表可自由缩放和排列，仪表盘布局可保存。
告警管理	集中展示系统的告警和事件，提供告警列表、事件列表、告警规则、告警通知等功能。 告警列表 告警是指AOM自身或外部服务在异常情况或在可能导致异常情况下上报的信息，并且您需采取相应措施清除故障，否则会由于AOM自身或外部服务的功能异常而引起业务的异常。

公共资源交易平台投标专用
AE2C13CEC77646E1A62A8B588EA14DB9

功能点	功能点描述
	告警列表展示已设时间范围内产生的告警。告警支持按照时间段、告警名称、告警源、告警级别进行过滤查询。 事件列表 事件告诉您AOM自身或外部服务发生了某种变化，但不一定会引起业务异常，事件一般用来表达一些重要信息。 事件列表展示已设时间范围内产生的事件。事件支持按照时间段、事件名称和事件源进行查询。 告警规则 通过告警规则可对资源的指标设置阈值条件。当资源的指标数据满足阈值条件时产生阈值告警，当没有指标数据上报时产生数据不足事件，以便您在第一时间发现异常并进行处理。 告警通知 通过创建通知规则设置告警通知策略，当AOM自身或外部服务存在异常或可能存在异常而产生告警时，可将告警信息以邮件或短信方式快速通知指定的人员，提醒相关人员及时采取措施清除故障，避免造成业务损失。
资源监控	提供应用监控、组件监控、主机监控、容器监控、指标浏览等功能。 应用监控 应用是您根据业务需要，对相同或者相近业务的一组组件进行逻辑划分，AOM提供以应用维度整体进行监控。 组件监控 组件即您部署的服务，包括容器和普通进程。组件列表展示了每个组件的类型、CPU占用、内存占用和告警状态等信息，AOM支持从组件下钻到实例，从实例下钻到容器。通过各层状态，您可完成对组件的立体监控。 主机监控 通过AOM您可监控主机的资源占用与健康状态，监控主机的磁盘、文件系统等常用系统设备，监控运行在主机上的业务进程或实例的

公共资源交易平台技标专用

功能点	功能点描述
	资源占用与健康状态。 容器监控 监控的对象仅为通过CCE部署的工作负载、通过ServiceStage创建应用。 指标浏览 展示了各资源的指标数据，您可实时监控指标值及趋势，还可将关注的指标添加到仪表盘，对其创建阈值规则和导出监控报告等操作，以便实时查看业务及分析数据。
日志管理	提供日志搜索、日志文件、日志转储、日志路径等功能。 日志搜索 当需要通过日志来分析和定位问题时，使用日志搜索功能可帮您快速在海量日志中查询到所需的日志，您还可结合日志的来源信息和上下文原始数据一起辅助定位问题。 日志文件 您可快速查看组件实例的日志文件，以便定位问题。 日志转储 AOM支持将日志转储到对象存储服务（Object Storage Service，简称OBS）的OBS桶中，以便进行长期存储。 AOM支持将日志转储kafka原始数据，且支持补全上下文信息。 日志路径 AOM支持容器服务日志和虚机（这里的虚机指操作系统为Linux的弹性云服务器或裸金属服务器）日志采集，即采集您自定义的日志文件并展现在AOM界面中，以供您检索。使用该功能前首先要配置日志采集路径。
配置管理	提供ICAgent管理、应用发现、日志配置等功能。 ICAgent管理 ICAgent用于采集指标、日志和应用性能数据。对于在ECS、BMS控制台直接创建的主机，您需手动安装ICAgent。对于通过CCE间接创

公共资源交易平台投标专用

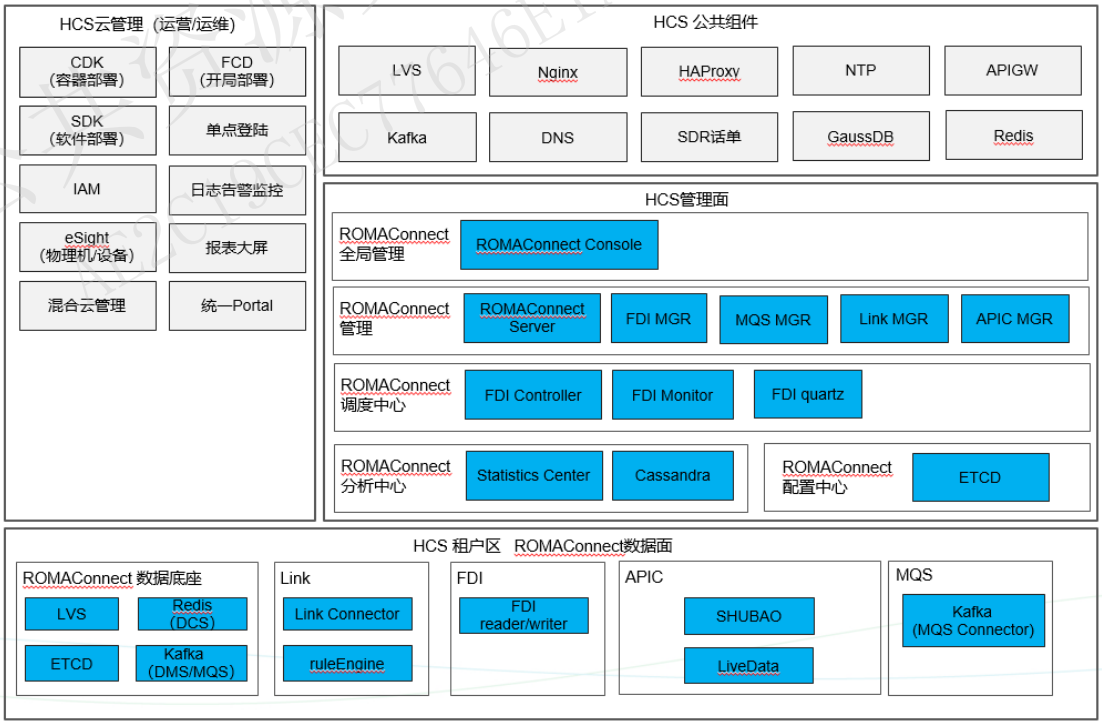
功能点	功能点描述
	建的主机，ICAgent会自动安装，您不用安装ICAgent。 应用发现 应用发现是指AOM通过配置的规则发现和收集您主机上部署的应用和关联的指标。 日志配置 提供日志配额和分词设置功能。 数据订阅 支持用户订阅指标或者告警信息，订阅后可以将数据转发到用户在ROMA Connect创建的 Kafka中，供消费者消费转发的订阅的信息。 若系统提示“验证规则失败”，请联系管理员检查环境配置。

AOM 特性列表

3.2.3.10.3 应用集成服务

3.2.3.10.3.1 系统架构

ROMA Connect 逻辑部署架构如下图所示：



ROMA Connect系统架构

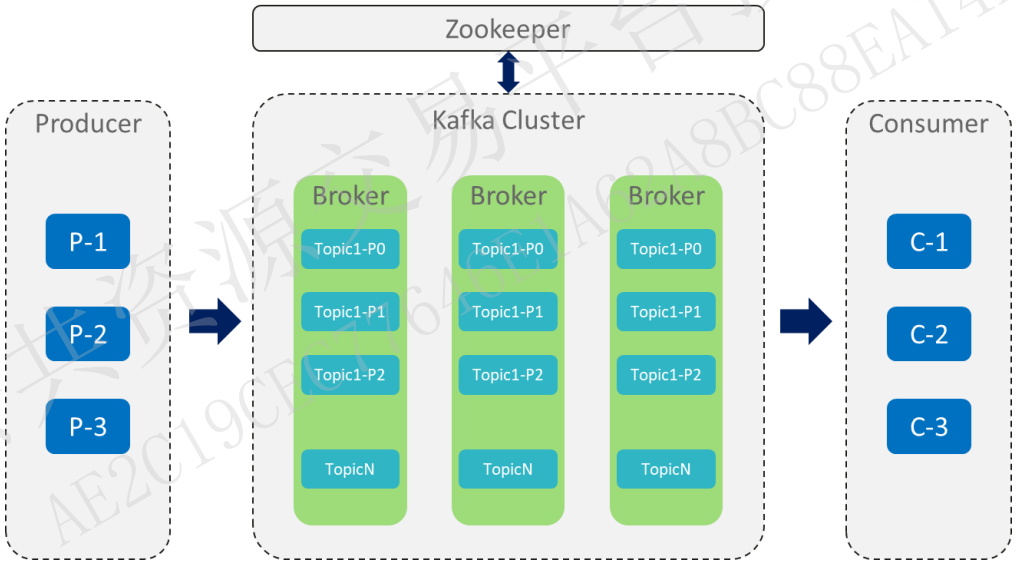
功能	说明
ROMAConnect全局管理	包含Console能力，可视化界面。
ROMAConnect管理	ROMA Connect生命周期管理，拆分为FDI、MQS等几个微服务进行管理
ROMAConnect 调度中心	包含FDI 控制器、监控、定时调度等能力
ROMAConnect 分析中心	分析API调用信息。
ROMAConnect 配置中心	存储用户创建的APP、API等配置信息
ROMA Connect数据面	包含数据底座，FDI、MQS等能力的Runtime。

ROMAConnect 组件列表

ROMA Connect 主要由 MQS、FDI、APIC 组成。

3.2.3.10.3.2MQS消息队列服务

提供跨网络访问的安全、标准化消息通道。



MQS系统架构

- Zookeeper：存储Kafka元数据。
- Broker互为主备
- topic按分区存储
- 副本分部在不同节点

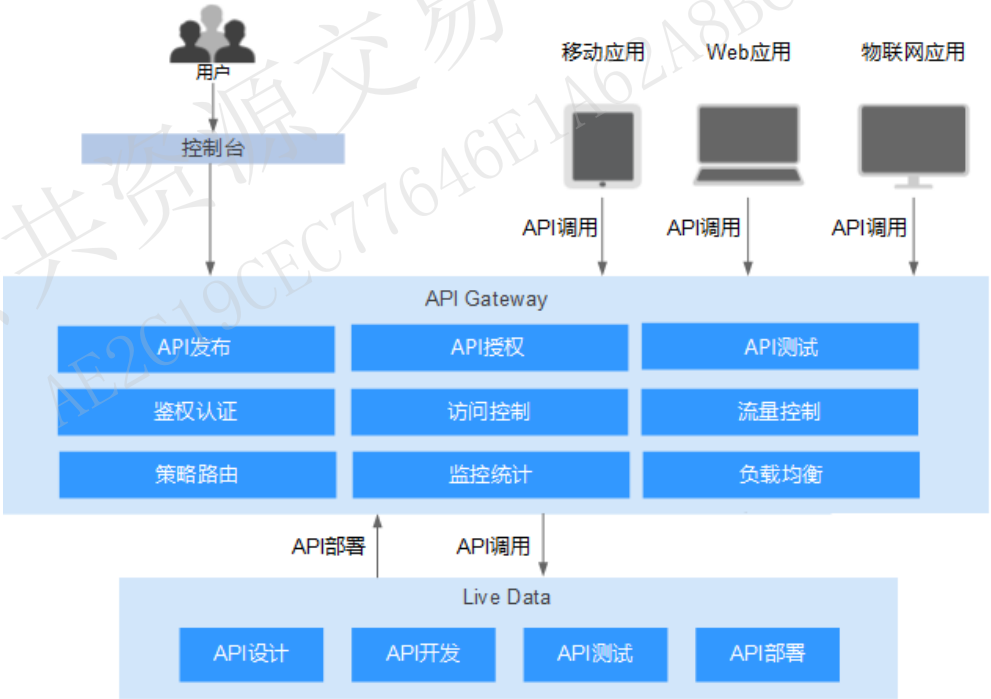
消息集成（Message Queue Service，简称 MQS）是 ROMA 平台的消息集成组件。MQS 基于 Kafka 协议，使用统一的消息接入机制，为企业提供跨网络访问的安全、标准化消息通道。

原生Kafka基础功能	MQS除了支持客户端连接后管理Topic和发布订阅消息，还支持在ROMA控制台可视化操作，包括Topic创建和管理、用户管理与权限设置、消息查询等功能。
监控报警	MQS从实例、节点、Topic、消费组等多个维度，设立了不同监控指标，数据上报华为云监控服务，企业可以在云监控服务的管理控制台查看相关监控数据。MQS支持企业配置告警规则，轻松实现监控数据概览与异常告警。
消息轨迹	MQS支持追踪消息生产与消费的完整链路信息，获取任一消息的当前状态，为排查生产问题提供有效数据支持。

MQS特性列表

3.2.3.10.3.3APIC 网关服务

API Connect，实现 API 全生命周期管理，将数据/后端服务以 API 形式开放。



APIG系统架构

服务集成 APIC（API Connect，简称 APIC）是 ROMA 平台的 API 集成组件。APIC 将数据和后端服务以 API 形式开放，简化分享数据或提供服务的过程，降低企业

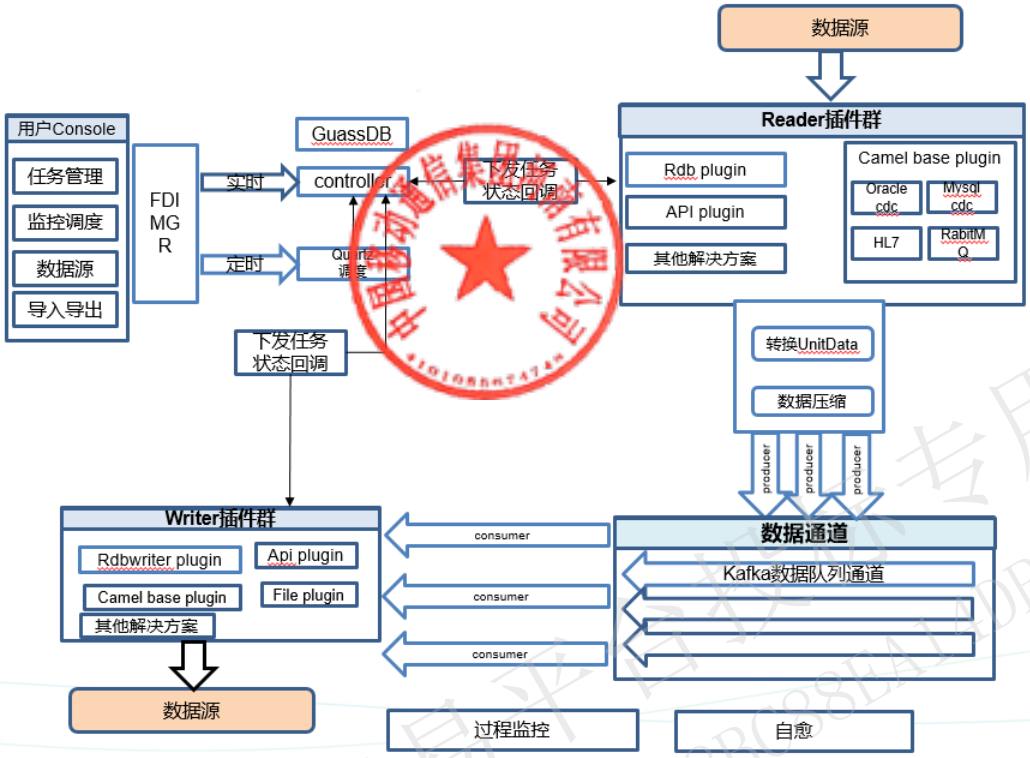
之间对接的成本。APIC 提供不同语言的 SDK 和示例代码，简化企业以 API 形式开放后端服务的过程。

API生命周期管理	APIC提供包括API的创建、发布、下线和删除的完整生命周期管理功能。
便捷调试工具	APIC提供页面调试工具，简化API开发，降低API的维护成本。
版本管理	一个API可以发布不同的版本到不同的环境，以满足业务版本升级等需求。
流量控制	用于管控API的请求频率、用户的请求频率和应用的请求频率。 流量控制的时间单位可以是秒、分钟、小时或天。允许设置特殊的应用，不受到流量控制策略的影响。
监控统计	提供实时、可视化的API监控，包括：API请求次数、API调用错误信息。
环境变量	当API发布到不同环境时，一般通过在API调用的请求头增加指定的头部参数及特殊取值区分不同的环境。发布过程中变量标识会根据环境的变量值进行替换，保证API本身定义不变。
自定义后端	包括自定义Data API与自定义Function API。 自定义Data API指企业将数据库作为API后端服务接入ROMA APIC，将数据服务能力转换为REST接口的能力。 自定义Function API，类似简化版的函数服务，在ROMA APIC后端编写自定义脚本或函数，作为API后端服务，供前端统一调用。
支持后端服务以域名方式访问	创建API时，后端服务地址支持填写域名。

APIC特性列表

3.2.3.10.3.4FDI数据集成服务

支持多种数据源之间的灵活、快速、无侵入式的数据集成。



FDI系统架构

（二）服务能力

ROMA Connect 源自华为流程 IT 的集成平台，在华为内部有超过 15 年的企业业务集成经验。依托 ROMA Connect，可以将物联网、大数据、视频、统一通信、GIS 等基础平台及各个应用的服务、消息、数据统一集成适配以及编排，屏蔽各个平台对上层业务的接口差异性，对上提供服务、消息、数据集成使能服务，以支撑新业务的快速开发部署，提升应用开发效率。适用于平安园区、智慧城市、企业数字化转型等场景。

- 支持多个ROMA Connect实例间的级联，可本地化调用其他ROMAConnect实例连接的服务域数据，“天涯若比邻”。
- 跨网过程中只需要维护维护、审计、监控唯一的ROMAConnect间数据管道，大大减低安全风险
- 支持多云、边云的应用、数据安全访问

公共资源交易平台专用

- 应用无需更改，非嵌入式对接
- ROMA Connect全域数据交换能力，总-分架构

快速数据集成FDI（Fast Data Integration，简称FDI）是ROMA平台的数据集成组件。FDI支持多种数据源（文本、消息、API、关系型数据和非关系型数据等）之间的灵活、快速、无侵入式的数据集成，可以实现跨机房、跨数据中心、跨云的数据集成方案，并能自助实施、运维、监控集成数据。

数据集成任务的生命周期管理	FDI支持修改数据集成任务的信息、查看数据集成任务的运行报告、查看数据集成任务的运行日志、查看数据集成任务状态，完成数据集成任务的生命周期管理功能。
系统管理	FDI提供权限管理、认证管理、菜单管理、用户管理等操作。
灵活的数据读写	支持 MySQL、文本文件、消息、API等多种数据的分片读取和写入。 如果服务意外中断 ，修复服务之后FDI支持自动修复任务。 支持任务调度、任务监控、任务中断续读。
可靠的数据传输通道	FDI可以持续监听数据通道中的数据，支持100个以上的线程并发执行。FDI实时监听消息队列把数据实时写入目标队列。
任务调度	FDI提供全面、灵活、高可靠的任务调度服务，支持通过API或以消息方式进行数据集成。按照时间、数据数量等任务触发规则来调度任务。根据任务配置，为插件分配任务，并监控和记录任务的执行状态。 企业根据不同的业务需求，可以选择不同的数据集成方式： 实时增量集成适用于需要实时监控数据变化的业务场景，例如收集生产线上设备的实时参数。 实时全量集成适用于需要实时监控所有历史数据的业务场景，例如统计供应商合作伙伴的出货量。

	定时增量集成适用于监控一段时间内数据变化的业务场景，例如企业采用新的生产策略后，验证生产效率是否达到预期效果。 定时全量集成适用于监控一段时间内所有历史数据的业务场景，例如统计上下班高峰期内出入园区的车辆数目。
便捷的调试工具	FDI提供便捷的页面调试工具，测试数据源是否能够连通，简化数据集成开发，降低维护成本。
监控告警	对创建的数据集成任务的运行情况进行监控，并对异常的任务进行处理，保证业务正常运行。
版本管理	一个集成任务可以发布不同的版本到不同的环境，以满足场景变换、版本升级等需求。

FDI特性列表

3.2.3.11 网络及托管建设方案

按照机房建设相关国家规范，将南阳生产楼机房建设成分区明确，功能完备，符合标准的现代化机房。IDC 机房的总体建设在立足“满足现在、适应未来”的建设策略的基础上，综合考虑各系统的先进性、高可靠性、高安全性、可持续发展性、节能性、易管理维护性、开放性、实用性、均衡性。



1、基础设施：IDC机房需要具备大规模的场地及机房设施，包括高速可靠的内外部网络环境，系统化的监控支持手段等一系列条件的主机存放环境。这些基础设施能够确保服务器的安全、稳定运行，并提供充足的网络资源，保证数据传输的效率和安全性。

2、互联网带宽：网络托管服务是提供商提供高速、稳定的网络带宽，确保客户的网站、应用程序等能够快速、稳定地访问。

3、互联网IP：IP地址是互联网通信的基础。通过IP地址，计算机可以互相发现和识别，实现信息的传递和交流。在网络通信中，IP地址被用于标识发送方和接收方，确保信息能够准确到达目的地。通过路由表的配置和更新，网络路由器能够根据目的IP地址选择合适的路径，提高网络传输的效率

4、设备托管：机柜/服务器（租用托管）主要包括服务器机位式租用托管、独立整机柜租用托管、VIP定制化服务。IDC机房托管服务方案可根据企业和组织的需求定制解决方案，满足不同规模和应用场景的需求。这种灵活性能够让企业和组织更好地适应不断变化的市场环境和业务需求。

2、网络管理：IDC 机房托管服务方案提供快速安全的网络，同时提供对服务器监管、流量监控等网络管理方面的服务。这些服务能够确保网络运行的稳定性和安全性，同时能够及时发现并解决网络中出现的问题。

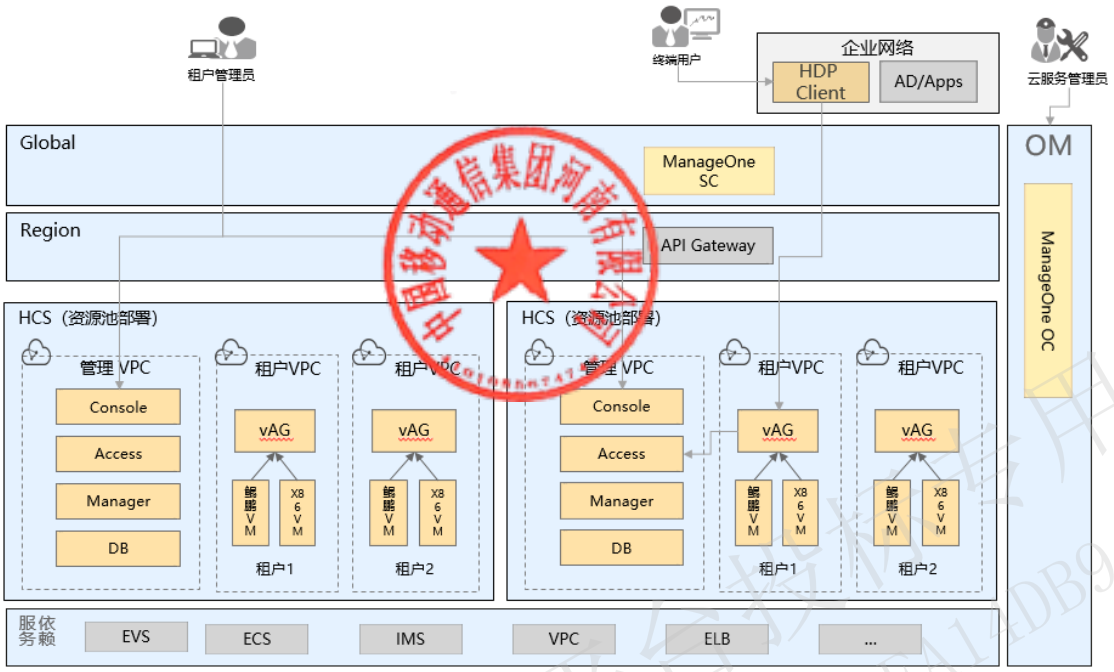
3、运维服务：IDC 机房托管服务方案提供 24 小时不间断的运维服务，包括故障申报、响应反馈、实时监控和应急措施等。这些服务能够及时处理服务器和网络中出现的问题，确保数据中心的稳定性和可用性。

4、专业支持：IDC 机房托管服务方案提供专业的技术支持和服务保障，包括技术咨询、系统维护、安全防范等方面。这些支持能够确保企业和组织的数据中心始终保持最佳状态，同时能够提高数据的安全性和可靠性。

3.2.3.12 云桌面建设方案

华为云桌面 Workspace 是一种基于 HCS 底座的安全、成熟的云计算应用，把原来分散在终端（PC）上的计算、存储等资源集中到数据中心，实现资源云化和集中管理，用户通过云终端（Thin Client 瘦终端、Software Client 软终端、Android 移动终端）接入网络中个人桌面进行数据和应用访问。Workspace 所拥有的海量算力、高可扩展、安全性、免基础架构运维、按需服务等特点，简化了软件、业务流程和访问服务，通过降低一次性成本和获取更大的灵活性操作，为政企市场带来更多可扩展的创新机会和 IT 能力。

3.2.3.12.1 系统架构



本项目为了实现高安全、高可靠、高性能、易远程集中运维、平滑扩容的目标，采用 Workspace on HCS 的方案，实现生产+办公一朵云部署。

本项目方案主要以下方面考虑：

资源池设计：根据本项目的需求，通过安装云平台系统软件实现硬件资源池的使能和操作。池化后服务器上运行虚拟机便于管理、监控。虚拟机可以实现定制策略迁移、手动热迁移、故障热迁移。资源池的设计具有高可靠、平滑扩容特性。

桌面云软件 Workspace：华为桌面管理软件 Workspace 能够提供高性能且可靠的桌面投送。桌面支持 Windows OS/银河麒麟桌面 OS/UOS。办公软件支持 WPS、永中 Office 等软件。Workspace 桌面虚拟化以华为云 Stack 混合云为基础，允许多个用户桌面以虚拟机的形式独立运行，同时共享 CPU、内存、网络连接和存储器等底层物理硬件资源。这种架构将虚机彼此隔离开来，同时可以实现精确的资源分配，并能保护用户免受由其他用户活动所造成的应用程序崩溃和操作系统故障的影响。

Workspace 采用业界领先的高清保真 HDP 桌面协议，并可将授权用户安全连接至集中式虚拟桌面。它与华为云平台协同工作，可提供桌面云，此方案不仅能

增强控制能力和可管理性，还可以提供与 PC 一致的桌面体验，Workspace 能简化虚拟桌面的管理、调配和部署。用户能够通过 Workspace 安全而方便地访问虚拟桌面，升级和修补工作都从单个控制台集中进行，因此可以有效地管理数百甚至数千个桌面，从而节约时间和资源。混合桌面云具备下列优势：

- 集控制能力和可管理性于一身：由于桌面在数据中心运行，因此管理员可以更轻松地对其进行部署、管理和维护。
- 桌面云把数据、信息和知识财产永保留在数据中心内，而且永远不外流。
- 与 PC 一致的体验：用户可以灵活访问与普通 PC 桌面功能相同的个性化虚拟桌面。
- 降低总体拥有成本（TCO）：桌面虚拟化可以减低其管理和资源成本。
- 统一软硬件管理：为了便于硬件设备（服务器、存储、交换机）、虚拟资源的集中管理，可使用华为云 Stack 平台。平台采用 B/S 架构，可以远程统一管理本项目中 VDI 桌面和计算资源池。支持管理虚拟机资源；支持虚拟机的快速部署、定制化策略调整
- 计算资源池

  计算资源池为用户提供 CPU、内存计算资源。在服务器上安装华为云软件，可以在一台服务器上虚拟出多个台虚拟机，提供弹性规格的虚拟桌面。这几个资源池归属同一朵云管理系统。

- 存储资源

存储资源主要为虚拟桌面提供系统空间和数据空间、还有云桌面管理系统所需要的空间。这里的数据类型主要包括：管理数据、虚机系统数据、用户数据。

终端：为用户提供虚拟桌面的键鼠输入、显示输出等交互能力。瘦终端 TC 或软终端 SC 通过桌面接入网关代理访问对应的虚拟桌面，终端、代理网关以及虚拟桌面之间采用 SSL 加密的 HDP 协议进行信息传递，并且可以通过策略开放或者禁止 TC/SC 等终端的 USB 外设权限，实现端到端的数据安全和可控。

用户通过在 TC/SC 上输入域用户名和密码访问对应桌面，终端形态上支持手机、Pad 移动设备，PC、笔记本固定终端以及瘦终端、会议白板等。接入网络上，既支持企业内部局域网访问和外部通过 VPN 加密通道访问，也支持 4G/5G、WiFi、

公共资源交易平台投标专用

互联网接入场景，进行移动远程办公。

3.2.3.12.2 服务能力

华为云桌面 Workspace 是基于华为云 stack 构建的云桌面服务，支持云桌面的快速创建、部署和集中运维管理，免除大量的硬件部署和维护投入。

云桌面可按需申请轻松使用，便捷调用云上的各种服务，实现配置动态变更、资源水平扩展，在线持续演进等能力，助力企业打造更便捷、更安全、更低维护成本、更高服务效率的 IT 办公系统。

- **简单高效**

  部署简单：企业使用传统电脑办公，一次性购买成本高，软硬件更新换代快，配置升级/变更繁琐，一般 2-3 年就会面临淘汰风险。华为云桌面是即买即用，可根据需求灵活申请和调整桌面的 CPU、内存、磁盘等规格，分钟级部署。

  运维高效：免除硬件运维，让客户运维更聚焦于业务效率提升。用户的资源、权限、运维统一管理，从线下分散运维变为云端统一运维，问题响应速度和效率提升，大大降低运维工作量。通过标准化模板支持用户操作系统、业务应用的统一化、标准化，实现 IT 办公平台的归一化管理。

- **安全可靠**

  病毒攻击、信息泄露、非法访问、数据监听等办公安全问题几乎是所有企业的困扰，尤其远程办公已成为刚需。华为云桌面具备接入终端、传输管道、云平台三大环节安全机制，10 项关键措施，实现数据不落地，规避企业办公中的各类数据安全风险。同时，通过多重强管控的安全策略，如显式/隐式桌面水印、外设管控、文件传输管控等，大幅减少信息泄露和安全隐患。

- **移动协同**

  不受限于办公地点，员工可随时随地通过登陆华为云桌面访问办公空间。笔记本电脑、Pad、手机、会议白板等设备均可登陆，一键直达办公空间。应用响应不依赖于终端的处理能力，而是直接利用云端桌面服务器的

公共资源交易平台投标专用

优越性能，大幅提升应用处理速度和用户体验。通过华为云覆盖全球的网络，在丢包<5%的不稳定情况下，仍可保证流畅办公体验。

- **高清流畅**

  电商、游戏、工业仿真、服装设计等行业对办公终端的显色真实度有很高的要求。通过**华为 HDP 高清传输协议（HUAWEI Delivery Protocol）**，华为云桌面能够为用户带来高清视觉享受下的流畅办公体验，保障 YUV444 真彩无损显示、专业 10bit 色深、柔滑细腻、4K/60 帧高动态场景流畅。

除了具备数据安全、访问便捷、部署灵活、运维管理等云桌面普遍具备的优势外，基于华为在电信行业的语音、视频、图像处理等领域 20 年的技术积累，以及服务政企客户的实战经验，华为云桌面更懂企业客户需求，通过先进的技术提供更优的服务。

【全自研桌面协议】华为云桌面是华为推出的基于公有云的云原生桌面 SAAS 化服务，并采用全自研的 **HDP（HUAWEI Delivery Protocol）高清传输协议**来实现高效的桌面远程连接，**拥有完全自主知识产权，100+专利，提供更优体验，更强的二次开发能力**。HDP 从 2013 年开始自研并商用至今，共服务了 4000+客户，250W+桌面，连续多年获得中国桌面虚拟化市场第一。

相对比于传统的桌面协议，HDP 具备以下特点：

1. 支持 32 条虚拟通道，每个虚拟通道可以承载不同的上层应用协议。
2. 采用动态压缩算法，对非自然图像采用无损压缩，对自然图像采用有损压缩，在带宽和显示效果之间取得最佳均衡。
3. 自动识别 VOIP 场景和音乐场景，采用不同的编解码算法，提升用户体验。
4. 支持多种协议的外设，主要包括 USB、打印机外设等；设立生态实验室，可快速支持客户或 ISV 完成新外设的适配验证。
5. 丰富协议管理策略。

【高清的办公体验】华为云桌面适配不同应用场景（普通文本、自然图像、视频、3D 图形等）采用不同压缩算法。最高支持 YUV444 真彩显示、专业 10bit 色深、4K60 帧视频播放。

1. 非自然图像采用无损压缩：自动识别整幅图像中的文字、Windows 图框、线条等非自然图像，对非自然图像采用无损压缩；相片、图片等自然图像采用合适的压缩率进行有损压缩（人眼对文字最敏感）。
2. 重复图像数据不传输：自动识别图像中的未变化部分，只有变化的部分数据会传输，极大降低带宽。
3. 支持多种图像压缩算法：可以根据不同的图像特点和场景选择最优的压缩算法。

【流畅的办公体验】华为云桌面根据不同场景自动选择最佳的优化手段，能在确保显示效果的前提下，同时又提高压缩率、降低压缩资源消耗和压缩时间。通过持续的策略优化，降低数据流各个环节的时延（如键鼠采样、图像编码、数据传输、图像解码等），同时利用华为覆盖全球的网络，通过就近接入、路径优化等能力降低网络时延，可实现用户键鼠操作至屏幕显示的时延小于 100ms（网络往返时延要求小于 20ms）。

【丰富的策略管理】华为云桌面在策略管理及外设支持方面，提供显示、音视频、水印、文件重定向等更丰富的功能选择，以满足客户多样化的需求。

1. 策略创建：支持新建、复制已有策略，复制模板创建。策略模板有默认 4 大场景推荐模板，可新建自定义模板，模板支持复制。
2. 音视频策略控制：支持设置播音、录音等详细参数。
3. 文件剪切板策略控制：支持设置本地磁盘映射关闭/只读/读写，支持设置允许的驱动器类型，支持设置流控；剪贴板关闭/只读/读写，支持设置允许剪切板富文本/文件。
4. 接入/会话策略控制：支持设置锁屏一定时间注销或断开。支持设置客户端自动重连间隔时间。
5. 默认策略：支持默认策略，默认应用于所有桌面，默认策略优先级最低。支持修改策略内容，不可删除。
6. 策略应用对象：支持桌面、用户、用户组（API）、终端 IP、OU（API）。在策略管理中指定策略应用对象，可以同时有多个/多种对象。不支持创建桌面指定策略。

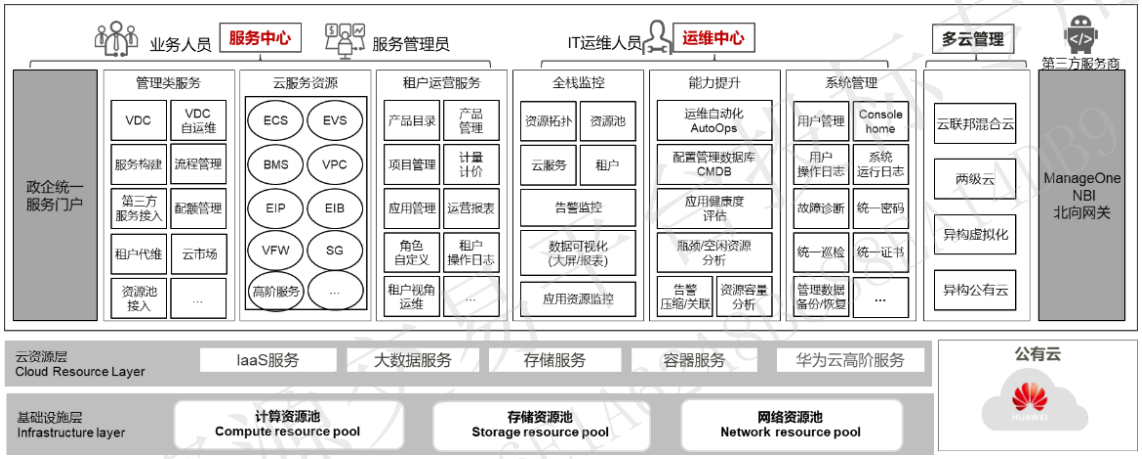
7. 外设：支持 USB、串口、并口重定向，支持 Twain/摄像头/PCSC 重定向。

【支持国产化场景】华为云桌面支持 ARM 桌面和 ARM 终端，支持国产化场景。

3.2.3.13 **云平台管理建设方案**

3.2.3.13.1 方案概述

ManageOne 在解决方案中承担 CMP（Cloud Management Platforms）的职责，通过自研和集成的方式，为云平台提供自租用的资源统一管理的能力，包括租户自助服务界面，云服务管理和服务目录，计量，计算、存储和网络资源自动化配置，云服务和云资源的运维监控、容器，虚拟机的统一管理和编排能力等。



云管理平台架构

ManageOne 解决方案包括运维中心 OC、云服务中心 SC、云系统运维 CloudScope lite。

运维中心 OC：云运维管理包含集中告警、统一监控、运维可视化、操作运维中心、日志中心等功能模块，支撑日常运维、系统变更、运营分析等运维业务场景，实现多个数据中心与混合云的集中运维管理。

云服务中心 SC：云服务中心包括产品目录管理，订单管理，用户/角色管理，配额管理，计量计价管理，流程审批等功能模块。支撑运营管理员的管理操作，以及普通租户的资源的自助申请和管理，实现多个数据中心，多类型资源池，多类型云服务的集中运营管理。

云系统运维 CloudScope lite：云系统运维包括 BaseLien，CAC 自动变更，SDK、CDK，统一配置 DCM 等功能模块。支撑 EI 服务，数据库服务，应用平台服

务，安全等服务的安装部署和升级操作。

ManageOne 南向接入不同类型的资源池、云服务、设备管理系统，提供统一服务发放和服务保障功能；北向提供开放 API，可以供第三方运营/运维/应用系统进行调用。

ManageOne 周边对接系统说明：

分类	说明
上级网管系统 第三方应用	ManageOne提供向上的接口，能够实现与上级网管系统的无缝集成，并支持接入运营系统或第三方应用等，提供用户需要的数据信息。
云服务	提供计算/存储/网络/大数据/PAAS/EI等多种云服务的申请发放能力，上报给ManageOne云服务实例的告警性能和资源信息。
FusionSphere OpenStack	统一提供完整的计算资源、存储资源和网络资源等管理服务，收集虚拟资源池的告警、性能、资源等监控数据，并汇聚上报到运维中心。
eSight	提供对云服务所依赖的基础设施的全方位监控，收集基础设施的告警、性能等监控数据，并汇聚上报到运维中心。
基础设施	包括计算（如服务器）、存储（如存储阵列）、网络（如交换机）。

ManageOne周边系统对接

3.2.3.13.2 统一门户

ManageOne 作为云的统一管理平台，将为云平台提供统一的管理入口以及门户管理，包括统一的自助服务门户、运营中心门户、运维中心门户。

（一）自助门户

ManageOne 提供开箱即用的默认服务目录，同时，IT 管理员可以按企业使用场景的需要添加服务分类、修改已有服务分类名称、修改云服务归属的服务分类、修改云服务在服务分类中的显示次序。

服务目录由云服务在安装部署的时候注册到 ManageOne，服务目录中呈现各类服务，主要包括：

- 计算：弹性云服务器、裸金属服务器、镜像服务、云主机备份、云服务器容灾
- 存储：云硬盘、对象存储服务
- 网络：虚拟私有云、弹性负载均衡、VPN、虚拟防火墙、弹性IP
- 安全：安全指数服务、程序运行认证、安全态势感知、边界防火墙、数据库安全、合作伙伴服务
- 数据库：关系型数据库、分布式数据库中间件、数据复制服务
- 应用服务：应用与数据集成平台ROMA、应用管理与运维平台 ServiceStage、应用编排服务 AOS、分布式缓存服务 Redis、容器镜像服务SWR
- EI企业智能：智能数据湖运营平台、图引擎服务、数据仓库服务、云搜索服务、ModelArts、MapReduce 服务

IT 管理员可根据企业需要，自定义服务目录，包括：添加服务分类、修改已有服务分类名称、修改云服务归属的服务分类、修改云服务在服务分类中的显示次序，使得服务目录更符合企业的使用场景。

租户可以自运维提供本租户及下级租户的基础运维能力，供租户管理员使用。支持告警管理包括当前告警和历史告警，支持按告警级别、监控对象类型、告警名称过滤查询告警。

（二）运营门户

提供统一的运营能力接入规范，云服务按照规范进行接入开发，可以提供统一服务目录、租户管理、多级 VDC、订单管理、配额管理、计量统计等能力，从而实现云服务的统一运营管理。

1.租户管理：租户由运营管理员进行开通和维护，创建租户时，运营管理员可以为租户设置配额上限，租户内所有企业项目的配额之和不能超过租户配额上限。

2.多级 VDC：VDC 是与企业/组织层级关系相匹配的资源分配单元，系统为每个租户默认创建一个一级 VDC，VDC 内能够完成用户管理、企业项目管理、配额管理、产品定义、资源发放、服务保障等功能。运营管理员可以创建和维护各级 VDC，VDC 管理员可以在 VDC 内再划分多个子 VDC，灵活匹配用户的组织模型。

公共资源交易平台投标专用

3.订单管理：运营管理员和 VDC 管理员可以审批用户提交的订单。审批时，可以选择同意、驳回修改、拒绝并关闭、转他人审批，转他人审批只能转给有审批权限的用户。

4.配额管理：IT 管理员为各业务部门的 VDC 设置配额，控制各业务部门可以使用的资源池资源数量，VDC 用户申请资源不能超过 VDC 配额。

5.计量计费：运营管理员可以查看租户的计量计价汇总信息，支持按规格指标计量。按 VDC 粒度对资源的使用量进行汇总，计量周期以小时为单位

（三）统一运维门户

为云平台提供统一的运维通道，支持统一的告警管理、全量资源监控、资源分析、数据大屏展示、报表管理等。

1.告警管理：运维人员通过告警监控来监控、管理系统自身或管理对象上报的告警或事件。告警监控提供了丰富的监控和处理规则，还可以将故障通知给运维人员，帮助高效监控、快速定位和处理网络故障，从而保证业务正常运行。

2.全量资源监控：全量资源监控是对物理设备到租户应用的全方位集中监控，帮助运维人员了解不同资源对象的告警状态、运行状态等信息，识别资源运行过程中的风险隐患。当监控过程中发现异常时，可在统一的监控详情页面，集中查看资源的拓扑、告警、性能等信息，并对资源进行自动作业、运行日志下载、拨测等操作维护，逐步分析问题，辅助运维人员快速进行故障排查与处理。

3.容量管理：资源池分析是按区域/资源池/可用分区/主机组（集群）等多个维度对计算、存储和网络资源池进行监控，结合关键性能指标，持续评估资源池的容量和负载情况，以指导运维人员进行资源池监控、规划、扩容等活动，最终达到提高资源利用率的目的。

4.数据大屏：管理员可以通过自定义可视化部件，将性能、容量、资源等不同维度的数据通过曲线图、饼图、柱状图多种样式组合展示在不同的 Dashboard 中，也支持卡片、地图、文字、表、树、图片等多种方式，帮助管理员监控、演示和汇报。

5.报表管理：报表提供数据分析和统计图表展示能力，运维人员可直接在客户端根据业务需求，将多个维度与指标任意交叉组合，并通过灵活的数据过滤，快速聚焦关键数据，实现自助式运维分析、定期汇报等工作。

公共资源交易平台技标专用

3.2.3.13.3　统一运营管理

3.2.3.13.3.1 系统架构

运营服务中心是云管平台的资源、服务管理中心，支持多租户模式，租户自助申请服务、管理资源，支持服务流程合规检查，提升运营效率，包括：

1.多云管理：支持对多个 Region 的云服务进行统一运营管理，满足大型企业或组织跨地域运营混合云的需求，支持多云管理，包括华为云、华为虚拟化、VMware、腾讯云等。

2. 政企组织结构管理：匹配政企多级组织管理模型，满足各级组织灵活使用云服务资源的需求，同时支持政企 IT 项目管理，把项目预算转换成资源配额，管控各业务部门的云资源池使用量，使得各业务部门在预算范围内合理使用云资源。

3. 权限管理：提供不同的运营权限，包括预置权限和自定义策略，满足政企不同用户角色的权限控制需求。

4. 服务管理：提供开箱即用的服务目录，支持服务按租户、按部门上架、下架，同时支持按需构建服务，支持跨 region、跨云的组合服务编排，支持重新编排云服务的申请页面，服务申请客户化，助力政企数字化转型；

5. 资源管理：支持全局统一的资源中心，运营管理员、租户可以在一张资源视图内管理所有 region 的云服务资源，支持对资源进行监控、执行常用操作。

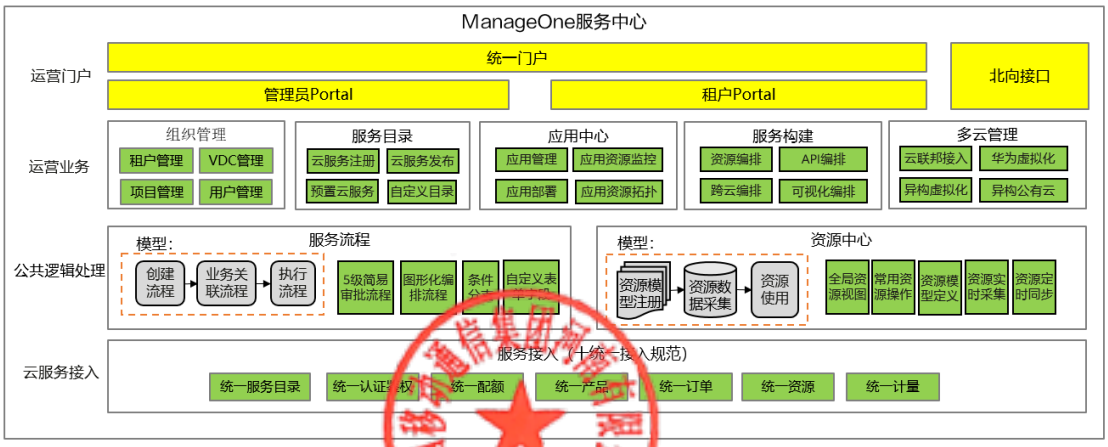
6. 应用管理：提供应用管理，政企的业务系统可以定义为应用，支持应用部署，以应用为中心管理云资源，提升运营管理效率；

7. 服务流程管理：提供图形化、按需定义的服务流程编排能力，可自定义服务流程（包括并行、串行处理）、流程节点、节点的表单定义，指定各节点的审批人，灵活适配各企业不同的业务审批诉求。

8. 运营管理：提供订单管理、配额管理、计量计价、购物车、回收站等运营能力，满足租户自助申请服务的诉求，提升运营效率。

运营服务中心在匹配政企组织管理模型的基础上，围绕服务、资源、应用的生命周期，结合统一服务流程进行合规管理。

公开资源交易平台投标专用



运营管理平台架构

1. 门户层：

统一门户：提供政企统一访问门户，门户支持预集成服务、动态构建注册的服务、ISV 开发的服务。

2. 运营业务层：

组织管理：匹配政企组织结构，提供企业、部门、项目不同层级的管理，通过部门配额控制各部门可使用的资源池资源数量，同时也可以通过项目预算为部门录入资源配额，管控各部门可以使用的云资源数量。

服务目录：支持服务按部门上架、下架，支持预集成服务、动态构建服务、ISV 开发的服务，支持多云服务的统一管理。

服务构建：支持按需构建服务，支持编排各原子服务 API、服务申请页面、申请流程，支持跨云服务编排，组合成用户需要的云服务，发布到服务目录，供租户自助申请使用。

应用中心：提供以应用为中心的资源管理，支持以应用为粒度管理、监控资源，支持在云主机上部署应用软件、应用模块进程监控，提供一站式的应用管理。

多云管理：支持接入多种云资源池，包括华为云、华为虚拟化、VMware、腾讯云等。

3. 公共逻辑处理层：

服务流程：提供服务申请、审批的统一流程，支持图形化可灵活定义的流程编排，支持定义流程表单。

资源中心：提供全局统一的资源管理中心，支持资源常用操作、资源监控，提供一站式的资源中心。

公开资源云管平台投标专用

4. 统一服务接入框架：

提供统一的服务接入框架，包括服务目录、鉴权认证、配额、订单、资源、计量。

3.2.3.13.3.2服务能力

（一）租户管理

租户是运营结算的独立主体，一般对应一个企业、集团/子公司：

1. 企业内部自用场景：全局创建一个租户，或者各事业部门对应一个租户。
2. 集团场景：总部、子公司各对应一个租户。
3. 出租场景（2B）：每个出租的企业对应一个租户。

运营管理员可以创建租户并且缺省给每个租户开通一个一级 VDC。

租户对应企业，租户中内置的多级 VDC（最多 5 级）对应企业不同部门，部门按照企业项目申请预算，再把预算换算成资源配额，通过企业项目的配额来控制各部门对云资源池的使用量。

租户由运营管理员进行开通和维护，运营管理员还可以在租户内创建和维护 1~5 级 VDC 以及 VDC 管理员。

租户（企业）在上云前如已经有认证系统，如 LDAP 认证，在开通租户时可以选择用户采用企业的认证系统，企业的认证系统需要提前在运营侧配置。

支持双因子认证，用户在登录时进行手机验证码二次验证，提高用户管理安全级别。

支持按租户设置费率，大客户可以采用不同的计费策略。

（二）多级 VDC

VDC 对应一个部门，用来匹配政企客户的多层级部门组织结构，最多支持 5 级 VDC。

VDC 是与企业/组织层级关系相匹配的资源分配单元，系统为每个租户默认创建一个一级 VDC，VDC 内能够完成用户管理、配额管理、项目管理、产品定义、资源发放、服务保障等功能。

VDC 可以按照组织来划分，一个组织分配一个 VDC，运营管理员创建和维护一级 VDC，但组织内可能存在多个子组织的情况，为满足多个子组织的需要，系统提供多级 VDC 功能，VDC 管理员可以在 VDC 内再划分多个子 VDC，灵活匹配用

公共资源交易平台技标专用

户的组织模型，VDC 可以支持 5 级 VDC 嵌套，每个 VDC 支持一个或多个 VDC 管理员。

运营管理员为 VDC 设置配额，可以控制各个部门可以使用的资源池资源数量，上级 VDC 管理员可以为下级 VDC 设置配额。

- VDC支持跨REGION。
- VDC支持为Region内不同云服务设置配额。
- VDC支持为不同用户关联不同的项目。
- VDC管理员可以将VDC业务员进行跨VDC映射project。
- 支持为VDC指定专属AZ。

（三）应用管理

应用对应租户的业务系统，租户可根据业务系统创建应用、把应用和资源关联、部署应用软件、提供应用 Topo、以应用的维度统计资源以及资源的性能负载、告警，并可以指定哪些用户可以管理应用。

应用管理支持如下功能：

1. VDC 管理员、VDC 业务员可以创建应用，VDC 管理员可以修改、删除 VDC 内的所有应用，VDC 业务员只可以修改、删除有权限的应用（包括自己创建的，以及被授权的）；

2. 运营管理员可以指定应用的审批流程（可选），指定审批流程后，VDC 管理员、VDC 业务员提交的应用创建申请需要审批；

3. 应用创建者就是应用管理员，他可以往应用添加、移除资源；

4. 应用管理员可以往应用添加人员，可以指定人员角色，包括应用管理员、应用实施人员，应用管理员有应用的所有权限，应用实施人员可以添加、移除资源、查看应用概览；

5. 应用管理员和应用实施人员可以为应用创建模块，给模块添加资源，指定模块进程的启动、停止、监控命令，后续应用管理员可以应用模块列表中管理模块进程。

6. 应用管理员和应用实施人员可以基于模块创建部署任务，完成应用软件的部署。部署任务支持立即执行，也可以在指定时间执行。

7. 应用管理员和应用实施人员可以在部署任务中添加部署步骤，在部署步

公共资源交易平台投标专用

骤中添加脚本，支持 shell 和 python 两种脚本。

8. 应用模块统计应用内资源的性能负载、告警，在应用概览中提供监控视图和应用模块 Topo，方便用户管理应用；

（四）服务管理

提供开箱即用的服务和服务目录，预置服务包括计算、存储、网络、数据库基础服务，同时提供容器引擎、大数据、应用服务等高阶服务。

运营管理员可按需发布服务给各 VDC，满足不同 VDC 的服务使用诉求。

（五）服务构建器

服务构建器是一个管理类服务，提供计算、存储、网络等云服务的组合编排、一键式部署以及基于监控指标的应用弹性伸缩功能。服务构建器支持跨 region、跨云资源（跨华为混合云和华为云）编排。

服务构建器支持两种编排模式：

一、资源编排

服务构建器提供图形化资源模板编排以及通过导入 RTS 模板编排、一键式应用部署、弹性伸缩的应用自动化部署服务。管理员和租户通过可视化编排界面任意拖拽图元或通过导入的 RTS 模板，快速完成计算，存储，网络，应用等资源的组合编排和自动化部署，并作为一个整体为用户服务，支撑业务快速上线。并且可以自定义自动伸缩策略以达到自动扩容和减容的弹性云服务器，以实现负载均衡，资源充分利用。

服务构建器的主要功能如下：

- 服务模板

服务模板是将计算、存储、网络、伸缩组、脚本等多种资源，按照特定关系的有机结合，基于服务模板可以快速构建服务并上线到服务目录。用户可以新建模板，也可以导入已有的模板，并支持 Heat 模板的导入。为了方便用户使用，缩短用户的学习过程，系统预置了大量常用的模板，包括：典型 Web 三层架构网站模板、安装 MySQL 服务模板、安装 MongoDB 集群模板、安装 Kafka 集群模板、安装 Nginx 服务模板、安装 Apache 服务模板、安装 Tomcat 服务模板等；

- 模板编排

服务构建器提供图形化模板编排功能。资源管理员可以在可视化界面通过拖

公共资源交易平台投标专用

拽图元的方式完成服务模板的设计、制作。可编排的元素包括弹性云服务器、网络、弹性负载均衡、脚本等元素，可设置各元素的信息和各元素之间的关联关系，编排完成后保存为模板。

- 服务构建

基于模板，可以构建服务并上架到服务目录。构建服务过程中，可以分类组合参数，锁定参数取值或开放出来由用户申请时指定。

- 服务实例化

服务上架之后，用户可以一键式申请服务并部署应用实例，系统根据模板定义创建服务实例、设置服务实例之间的关联并根据脚本自动部署应用软件，实现一键式应用部署。申请过程中，用户还可以指定服务实例归属哪个应用，也可以不指定应用，服务构建完成后自动生成一个应用，完成服务资源和应用的关联，便于后续基于应用管理资源。

- 部署脚本

编排服务模板时，可以指定在弹性云服务器上运行的脚本，通过脚本完成应用软件的安装部署。服务构建器支持三种应用软件部署模式：镜像、Cloud-init、脚本，脚本的部署方式最灵活，功能也最强大。系统支持脚本管理功能，用户可以将本地的脚本文件上传到系统，系统会将脚本信息保存到数据库中，后续使用模板发放实例时，可以选择已有的脚本。

二、API 编排

服务构建器支持 API 编排模式，可以通过服务构建器的 API 编排图形化设计器将接入的 IT 系统 API 在线进行 API 组合编排，在线设计申请服务的表单，基于此 API 编排模板快速构建服务并上线到服务目录，让政企原有 IT 能力“云化”重生，统一 IT 能力服务化流程，实现政企 IT 共享，丰富 IT 能力服务化生态。

服务构建器的 API 编排能力将现有 IT 能力组合编排在线构建新服务，解决政企现有 IT 能力服务化。

服务构建器应用场景：

1. 单云服务重编：通过服务构建器对原生云服务按需进行重新编排，解决原生云服务用户体验和政企 IT 申请流程适配问题，标准化申请流程，满足政企 IT 治理管控诉求。

公共资源交易平台投标专用

2. 多云服务混编：根据业务场景通过服务构建器将多种云服务进行混合编排，解决当前云服务功能化、细片化的问题，将各云服务原子化的能力按照客户场景进行编排，构建政企客户自己的“场景化云服务”。

3. 跨云混合联编：通过服务构建器将公有云的服务和私有云的服务联合编排实现跨云混合，根据业务场景灵活选择部署架构，合理利用资源，达成业务部署成本最优，解决客户资源及服务协同，简化用户体验及管理，打造客户视角一朵云。

4. 现有 IT 能力新编：通过服务构建器将政企 IT 服务的 API 根据业务场景在线组合编排，解决政企现有 IT 能力服务化，上架云服务市场和目录问题，让政企原有 IT 能力“云化”重生，实现政企 IT 共享，丰富 IT 能力服务化生态。

（六）服务流程

支持服务流程管理，预置常见审批模板，运营管理员和 VDC 管理员可按需自定义审批流程。

支持图形化定义审批流程，运营管理员和 VDC 管理员可通过拖拉拽的方式定义审批流程，支持串行、并行、会签等流程，可自定义每个流程步骤的参数表单，指定每一级的审批人，还可以审批用户组的方式批量指定审批人，满足不同企业的不同业务审批流程诉求。

除了图形化自定义流程之外，运营服务中心还提供简易的 5 级审批流程，运营管理员和 VDC 管理员都可以定义该审批流程，每一级可以指定一个或多个审批人，该级审批人员均有处理此订单的权限，任一审批人批准则本级审批通过。

审批流程创建后还需发布才能正式生效，运营管理员发布的审批流程，全局可见，VDC 管理员发布的审批流程，本级和下级 VDC 可见。

审批流程的修改和删除必须确保该流程处在未发布状态，已发布的审批流程需要先取消发布，并确保该流程未被任何产品关联。

云服务在上线时，如果明确该产品需要走审批流程，则可以在定义产品时关联已发布的审批流程。

云服务的申请，变更，加入回收站，从回收站恢复，删除，延期等操作，均可以关联不同的审批流程，也可以选择不审批，默认值为不审批。

（七）订单管理

公共资源交易平台投标专用

提供订单审批能力，可以选择同意、驳回修改、拒绝并关闭、转他人审批。

运营管理员和 VDC 管理员可以审批用户提交的订单。审批时，可以选择同意、驳回修改、拒绝并关闭、转他人审批，转他人审批只能转给有审批权限的用户。

支持查看整个审批流程和进展，已经通过的审批环节显示实际的审批人，待审批环节显示审批人列表，后续的审批环节不显示审批人。

支持多级审批，支持审批通知机制，系统在审批人审批后，可以根据邮件配置和审批消息配置发送通知。

运营管理员和 VDC 管理员，可以批量审批订单，可以选择同意、驳回修改、拒绝并关闭、转他人审批。转他人审批只能转给有审批权限的用户。

对于未审批的订单，提交人可以主动撤回订单。撤回的订单可以关闭，也可以修改后重新提交。

订单提交人可以查看自己提交的订单的审批进度。VDC 管理员可以查看本 VDC 内所有订单的审批进度。查看审批进度时，可以查看整个审批流程和进展，已经通过的审批环节显示实际的审批人，待审批环节显示审批人列表，后续的审批环节不显示审批人。

订单提交后，系统根据手机/邮件配置，给订单审批人发送通知消息。审批完成后，申请人收到实施结果的通知消息。

订单关联的服务实例到期前，通过短信和邮件通知提醒，到期后如果没有续期则每天提醒一次，直到删除或者延期为止。

（八）用户管理

服务中心的用户分为系统、代维、租户三种类别：

1. 系统：服务中心管理侧的用户。
2. 代维：代维用户，可以 VDC 管理员的身份管理多个指定的租户。
3. 租户：服务中心租户侧的用户。

系统预置运营管理员、VDC 管理员、VDC 业务员、VDC 只读管理员四个用户组：

1. 运营管理员：管理侧的用户组，用户类别为“系统”时对应的用户组。
2. VDC 管理员：租户侧的用户组，具有 VDC 管理权限和云服务管理权限，可以管理 VDC、申请/管理云服务，创建用户，选择用户类别为“租户”时，可以

选择 VDC 管理员用户组。

3. VDC 业务员：租户侧的用户组，具有云服务管理权限，可以申请/管理云服务，创建用户，选择用户类别为“租户”时，可以选择 VDC 业务员用户组。

4. VDC 只读管理员：租户侧的用户组，具有 VDC 只读权限和云服务只读权限，创建用户，选择用户类别为“租户”时，可以选择 VDC 只读管理员用户组。

当以上三种租户侧的用户组不能满足需求时，运营管理员、VDC 管理员也可以自定义租户侧的用户组，按需给用户组授予权限，创建具有不同权限的用户组。

把用户加入用户组，则用户具有该用户组的权限。

用户组的功能包括：

- 支持为用户组添加、删除用户。
- 支持为用户组添加权限。
- 支持为用户组关联资源集，可以关联一个或多个资源集。

（九）计量计费

按租户计量云服务资源使用，计量周期以小时为单位。

运营管理员可以查看单个租户计价信息，也可以查看租户下云服务的计价详情，支持查看按计量指标维度的计量和计价信息，同时支持查看计量指标对应云服务实例的计量计价详情。

租户内按 VDC 粒度对资源的使用量进行汇总，计量周期以小时为单位。

- VDC管理员可以查看本VDC和下级VDC计量和计价信息。
- 支持按区域、资源集、资源类型等多维度进行汇总计量计价。

租户计量计价数据可以通过报表功能导出，导出格式为 excel。

按资源规格定价，运营管理员可以为每种规格设置费率，如 1CPU2G 内存弹性云服务器为 1 元/个-小时。

系统提供通用计费方案费率设置和按租户设置费率功能，如租户希望有单独的费率设置，可用新增租户费率方案，，计量指标不变。

云服务类型	云服务名称	计量指标	计量单位
计算	弹性云服务器	弹性云服务器使用个数。	个-小时
	裸金属服务器	裸金属服务器使用个数。	个-小时
存储	云硬盘	云硬盘-容量。	GB-小时

公共资源交易平台投标专用

云服务类型	云服务名称	计量指标	计量单位
	云硬盘-快照	云硬盘-快照。	GB-小时
	对象存储	对象存储-存量。	MB-小时
		对象存储-外网流出流量。通过互联网从对象存储下载数据所产生的下行流量。	GB-小时
		对象存储-外网流入流量。通过对象存储控制台界面或通过互联网，上传数据到对象存储所产生的上行流量。	GB-小时
		对象存储-内网流出流量。弹性云服务器通过华为云Stack内网下载对象存储的数据所产生的下行流量。	GB-小时
		对象存储-内网流入流量。弹性云服务器通过华为云Stack内网上传数据（通过第三方应用或API进行上传）到对象存储所产生的上行流量。	GB-小时
		对象存储-请求总次数。	Number-小时
	弹性文件服务	弹性文件服务使用量。	GB-小时
网络	虚拟专用网络	VPN-个数。	个-小时
	带宽	弹性IP-带宽。	Mbit/s-小时
	弹性IP	弹性IP-个数。	个-小时
	弹性负载均衡	弹性负载均衡-个数。	个-小时
	虚拟专用网络-带宽	VPN-带宽使用量。	GB-小时

公共资源交易平台 招标专用
AE2C19CEC77C4621A62A81C88CA14DB9

云服务类型	云服务名称	计量指标	计量单位
	云专线	云专线使用个数。	个-小时
	NAT网关	使用个数。 指标包含： NAT网关-小型 NAT网关-中型 NAT网关-大型 NAT网关-超大型	个-小时
灾备	云服务器备份	使用容量。 指标包含： 云服务器备份-备份容量 云服务器备份-复制容量	GB-小时
	云硬盘备份	使用容量。 指标包含： 云硬盘备份-备份容量 云硬盘备份-复制容量	GB-小时
	云服务器容灾卷资源	容灾主机卷容量。	GB-小时
	云服务器容灾实例资源	容灾实例使用个数。	个-小时
	云服务器高可靠卷资源	高可靠主机卷容量。	GB-小时
	云服务器高可靠实例资源	高可靠实例使用个数。	个-小时
安全	边界防火墙	边界防火墙使用个数。	个-小时
	主机安全服务	保护虚拟机个数。	个-小时
	网页防篡改	标准版实例个数。	个-小时
	WEB应用防火墙	使用个数。 指标包含：	个-小时

公共资源交易平台技标专用

云服务类型	云服务名称	计量指标	计量单位
		基础版 标准版 高级版 旗舰版	
	密钥管理服务	使用个数。 指标为：CMK。	个-小时
	堡垒机	使用个数。 指标包含： 堡垒机旗舰版 堡垒机基础版 堡垒机标准版 堡垒机高级版	个-小时
	云数据库审计系统	使用个数。 指标包含： 数据库审计旗舰版 数据库审计基础版 数据库审计标准版 数据库审计高级版	个-小时
	综合日志审计平台	使用个数。 指标包含： 综合日志审计旗舰版 综合日志审计基础版 综合日志审计标准版 综合日志审计高级版	个-小时
	WEB防御及态势感知	使用个数。 指标为：基础版。	个-小时
	综合漏洞扫描	使用个数。 指标包含：	个-小时

公共资源交易平台投标专用

云服务类型	云服务名称	计量指标	计量单位
		漏洞扫描旗舰版 漏洞扫描基础版 漏洞扫描标准版 漏洞扫描高级版	
数据库	关系型数据库	关系型数据库-规格 关系型数据库-存储容量 关系型数据库-备份容量	个-小时 GB-小时 GB-小时
	数据复制服务	数据复制服务-规格 数据复制服务-存储容量	个-小时 GB-小时
两级云	云硬盘-快照（两级云）	云硬盘-快照（CRS）的使用量。	GB-小时
	虚拟私有云（两级云）	虚拟私有云（CRS）使用个数。	个-小时
	弹性IP（两级云）	弹性IP（CRS）使用个数。	个-小时
	弹性云服务器（两级云）	弹性云服务器（CRS）使用个数。	个-小时
	云硬盘（两级云）	云硬盘-容量（CRS）的使用量。	GB-小时

云服务计量指标1

云服务类型	云服务名称	计量指标	计量单位
融合资源池	云硬盘	云硬盘容量的规格。	GB-小时
	弹性云服务器	弹性云服务器使用个数。	个-小时
	虚拟防火墙	虚拟防火墙使用个数。	个-小时
	弹性IP	弹性IP使用个数。	个-小时
	弹性负载均衡	弹性负载均衡使用个数。	个-小时

公共资源交易平台投标专用

云服务计量指标2

由于云主机和云硬盘采用不同的介质将导致不同的服务质量，因此运营平台支持 SLA 的计量方式。如果有 SLA 配置则区分 SLA 定价（云硬盘根据磁盘存储 SLA 磁盘类型进行计价）。

资源对象	定价资源	单位	单价（举例）
弹性云服务器	弹性云服务器-CPU	个-小时	0.5 元
	弹性云服务器-高性能CPU	个-小时	1 元
	弹性云服务器-内存	GB-小时	0.2 元
云硬盘	云硬盘-容量-SATA	GB-小时	0.1 元
	云硬盘-容量-SAS	GB-小时	0.1 元
	云硬盘-容量-SSD	GB-小时	0.2 元

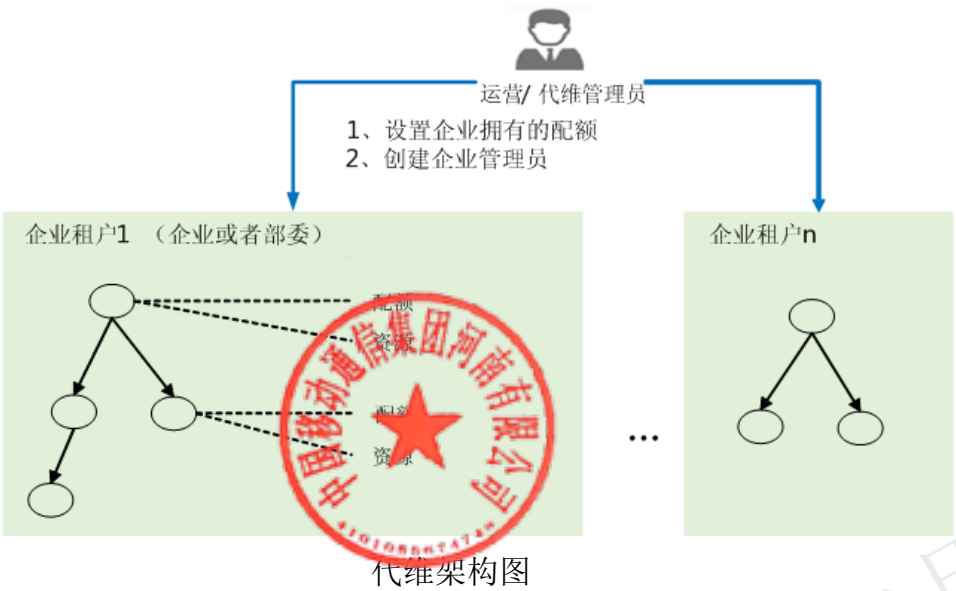
云服务计量指标3

用户对资源不同的操作产生计量数据。比如虚拟机：有创建、修改、开机、关机、删除，记录各操作时间段，在云服务侧生成多条离线话单记录，组成离线话单文件。系统根据离线话单文件记录的计量信息进行业务结算。提供计量 API，客户计费系统可通过计量 API 获取计量数据进行计费。

（十）代维管理

支持运营或代维管理员跨一级 VDC 代维，代维账号可以进入被代维的多个一级 VDC 进行代维。跨一级 VDC 代维，支持创建、删除、修改代维管理员。代维管理员可以进入被代维的多个一级 VDC，代替 VDC 管理员进行 VDC、用户及资源等的管理。

公共资源交易平台技术专用



代维架构图

- 运营管理员根据企业组织结构设置各部门，设置各部门资源配额
- 运营管理员通过部门切换，为各部门申请资源，并通过线下方式将资源信息通知最终使用者
- 资源最终使用者并不登录云管平台
- 运营管理员代维申请的资源，占用申请部门的配额

（十一）购物车

产品申请过程中，对于同一类型的产品，用户可以一次申请，但是对于不同类型产品，用户需要分别申请，不能多个产品一次提交申请，对于已经填写好规格参数的产品，若没有提交申请，后续申请时需要重新从产品列表中选择该产品并填写参数后才能申请，增加了用户申请的操作时间。

通过购物车功能，用户可以实现：

1. 将不同类型的产品添加到购物车，通过购物车一次申请。

2. 对于已经添加到购物车的产品，用户前期没有申请，后续可以直接在购物车中提交申请，无需再次从产品列表中选择需要的产品申请。

3. 通过购物车提交申请时，可以填写相关的补充信息如合同号和附件。

同时，在购物车还提供产品的移出或产品申请时长、规格的修改功能。

（十二）回收站

支持用户删除资源后保留到回收站，允许误删除后恢复资源，支持资源冻结期设置，在冻结期内不允许彻底删除。

公共资源交易平台投标专用

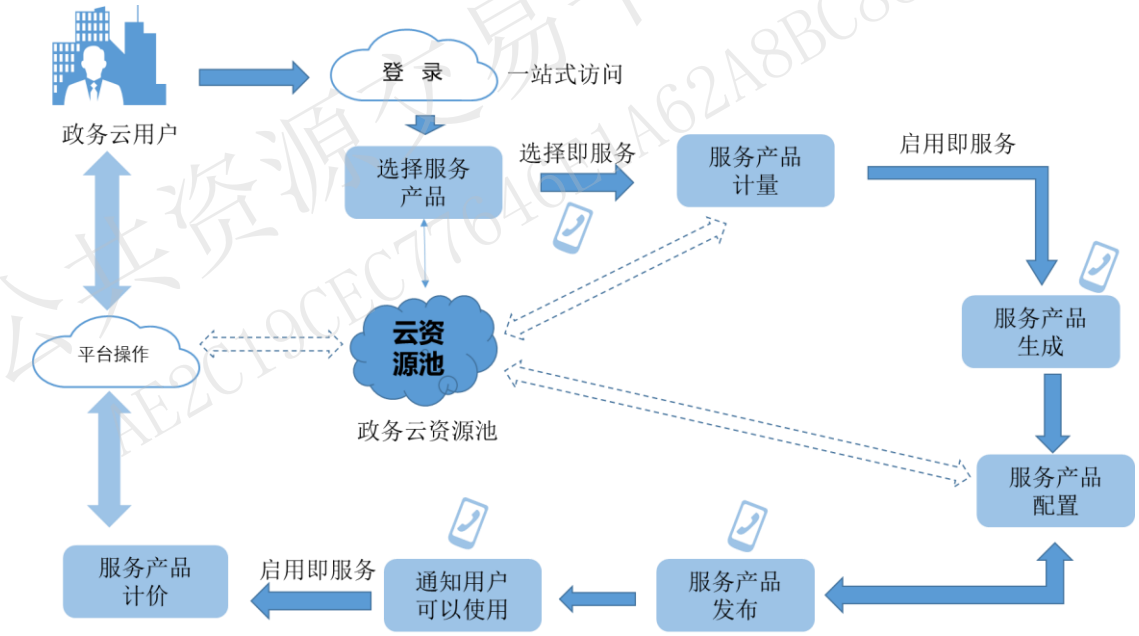
3.2.3.13.3.3云管理平台功能

提供统一云管理平台，支持业务快速上线，同时提高基础架构的自动化管理水平，确保满足基础设施快速适应业务的敏捷诉求，用户可以使用该平台提供的服务，包括云主机、云硬盘、云防火墙、云网络、云数据库、公网 IP 等服务。支持不同的角色：云管理员、组织管理员、用户，实现对不同角色的授权，不同的角色具有不同的访问权限，并且支持多租户的组织管理，云管理员可以对组织进行创建、修改、删除等操作。

3.2.3.13.3.3.1 **自助式服务门户**

为用户提供自助式服务门户，用户可以自行登录服务门户，使用云运营管理平台提供的服务。

自助式服务门户在 IT 服务管理中起着举足轻重的作用，是信息中心和用户沟通的主要桥梁，事件管理的故障主要来源，系统单独为服务台的角色创建了相应的服务台模块让服务台可以更加方便的处理日常的工作事项。



门户登录：用户可以自定登录服务门户，系统提供用户安全认证等登录保障

服务目录：提供用户查看当前已申请的各类服务的总列表，例：目前申请的虚拟机数量、存储数量，以及配套的运维保障、原厂服务等。

任务箱：提供用户查看当前的任务消息，包括各类告警信息、订单执行信息、服务审批结果等

公告栏：展示当前平台的各类公告信息

仪表盘：提供用户查看关注的各类统计图表，可选展示个人资源健康度图表、计费计量统计表等各类统计图表

系统管理：提供用户、角色、权限、日志、数据、安全相关的后台配置管理服务。

3.2.3.13.3.3.2 **云主机服务**

提供云主机服务，用户可以自助选择镜像类型、虚拟机规格、网络、计算/存储等申请虚拟机。支持将虚拟化平台的虚拟资源定义成服务目录供用户申请使用。

提供弹性云服务器服务，具备兼容 X86、ARM、GPU 等架构服务器能力，支持 IPV4/IPV6 双栈，支持虚拟机的亲和性和反亲和性，支持云服务器的个性化初始配置，当用户申请云服务器时，可以同时分别设置每块数据盘的容量以及每块网卡的网络。

支持用户申请虚拟机时即为虚拟机配置虚拟机的亲和性和反亲和性。在同一个反亲和性组中的虚拟机将尽可能分布在不同主机上，满足虚拟机的可靠性保障要求；在同一个亲和性组中的虚拟机会将虚拟机尽可能放在相同主机上，满足虚拟机启动相关性要求。支持用户查看每个亲和/反亲和性组中的虚拟机。

支持云服务器的个性化初始配置，支持用户申请弹性云服务器时增加数据盘以及网卡，可以分别设置每块数据盘的容量以及每块网卡的网络。

3.2.3.13.3.3.3 **云硬盘服务**

提供云硬盘服务，支持用户自助申请云硬盘，并挂载给虚拟机。云管理平台中管理虚拟化平台的存储资源时可以根据 SSD/SAS/SATA、IOPS 等参数配置不同的存储资源池（如高速、中速、低速等类型），用户申请存储资源时可根据需要选择对应的资源池，达到云存储规格分级管理与使用的需要。

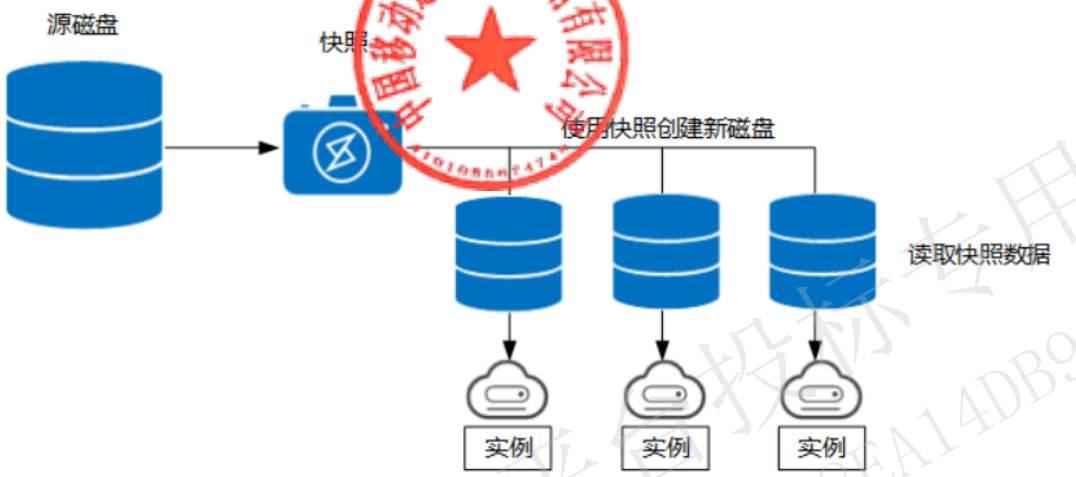
提供云硬盘服务，支持共享盘、SCSI 指令透传，具备云硬盘快照创建、扩容、卸载、删除、快捷查看、搜索等云硬盘便捷管理功能，支持用户通过自助维护界面完成云硬盘 SLA 变更能力。

云硬盘服务提供多样化持久性存储设备，用户可灵活选择磁盘类型，并自行在磁盘上进行文件存储、搭建数据库等操作。云硬盘服务主要功能特性如下：

（1）云硬盘快照创建

用户可以基于快照创建新的云硬盘，这样云硬盘在初始状态就具有快照中的数据，是原始云硬盘的精确副本，通过快照创建的云硬盘不需要再进行分区、格式化及创建文件系统等操作，挂载到实例后就可以正常读写快照上的所有数据。因此，快照是数据共享和迁移的重要方式。

通过同一个快照可以快速创建出多个具有相同数据的云硬盘，从而可以同时为多种业务提供数据资源。



（2）支持弹性挂载/卸载

云硬盘服务磁盘就像原始未经格式化的外部数据块存储设备，可挂载到单个实例。磁盘始终不受实例运行时间的影响。将磁盘挂载到实例后，用户可以像使用其他物理硬盘一样使用它。用户也可以将磁盘从实例中卸载，并将其挂载到另一个实例。

（3）支持多种磁盘类型

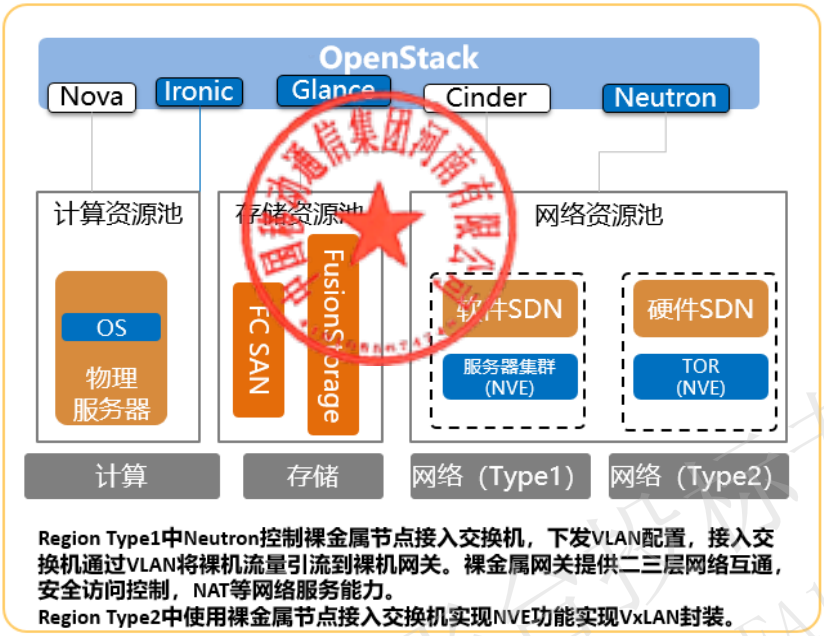
一个磁盘类型对应一组磁盘所使用的后端存储。用户可以根据接入的不同后端存储类型划分云硬盘的磁盘类型，以便满足业务不同性能要求。当业务与所在存储的读写性能配置不匹配时，用户可以通过变更磁盘类型调整磁盘所在存储介质的类型来改变读写性能，以应对实例存储业务性能调整的诉求。

3.2.3.13.3.3.4 物理服务器服务

提供物理服务器服务，支持将物理服务器定义成服务目录供用户申请使用，用户可以根据自己的需要选择镜像类型、物理机规格、网络、系统，由云服务商完成服务器的操作系统安装、网络配置。

BMS（Bare Metal Server），即裸金属服务器，为租户提供专属的物理服务

器，拥有卓越的计算性能，能够同时满足核心应用场景对高性能及稳定性的需求，并且可以和虚拟私有云等其他云服务灵活的结合使用，综合了传统托管主机的稳定性与云上资源高度弹性的优势。



3.2.3.13.3.3.5 **云服务能力**

云管理平台能够通过自服务门户能够为用户提供云主机、云硬盘、云防火墙、云负载均衡等服务。

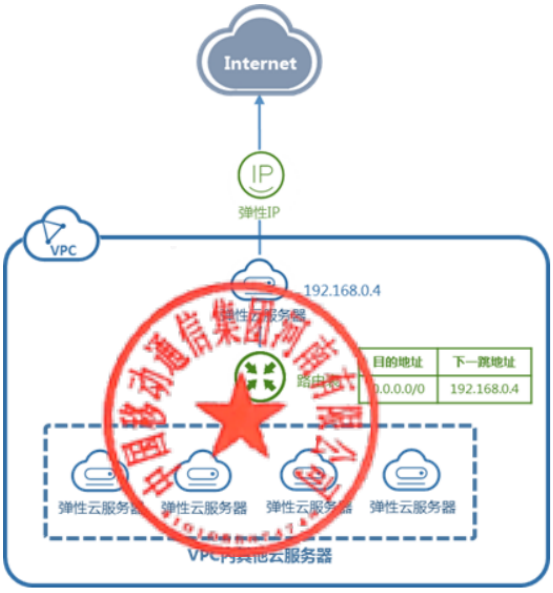
3.2.3.13.3.3.6 **VPC（虚拟私有云）服务**

提供 VPC（虚拟私有云）服务，支持向 VDC/租户提供独享的、同其它网络逻辑隔离的虚拟网络，拥有独立的地址空间。支持按业务需要自助创建 VPC 内的网络业务，包括子网、VRouter 等。支持用户规划自己的私网地址，不同的 VPC 之间的 IP 地址可以重叠。

提供虚拟网络环境能力，支持用户自助创建私有的隔离的虚拟网络环境、通过云平台自主管理不同隔离的网络环境的互通规则，具备 VPC 下子网管理能力。

用户可以在虚拟私有云内自定义私有网络网段、子网网段和路由策略，根据需要将云服务器和其他服务部署在对应的子网下。

公共资源交易平台技术专用



支持用户自助创建私有的隔离的虚拟网络环境，每套隔离的虚拟网络环境可以包含一套虚拟的出口路由器和若干虚拟防火墙以及子网网络。用户可以完全掌控自己网络环境，包括支持自助创建子网，指定子网网段、掩码，子网使用的 DNS。

支持用户通过云平台自主管理不同隔离的网络环境的互通规则，用户可以配置不同网络环境之间的三层互通规则，可以配置允许不同的网络环境之间不同的子网是否可以通过三层互相访问；已经配置了可以三层互通的，可以自助取消三层互通。

支持用户申请专线服务，实现 VPC 中子网和云外网络互通，支持用户申请时指定网络打通时使用的物理专线、虚拟网关、远端子网等。

3.2.3.13.3.3.7 **负载均衡**

具备通过流量分发扩展应用系统对外的服务能力，提高应用程序的容错能力。

支持 4 层、7 层负载均衡，包括 HTTP、HTTPS、TCP、UDP 协议的监听。

支持会话保持，将相同来源的访问转发至同一后端服务器，7 层监听需支持基于 cookie 植入和重写两种方式。

HTTP(S)协议的监听支持源 IP 透传，将访问来源 IP 透传给后端服务器。

支持基于 TCP、HTTP、UDP 协议的健康检查，基于 HTTP 协议的健康检查支持自定义域名和 URL 路径。

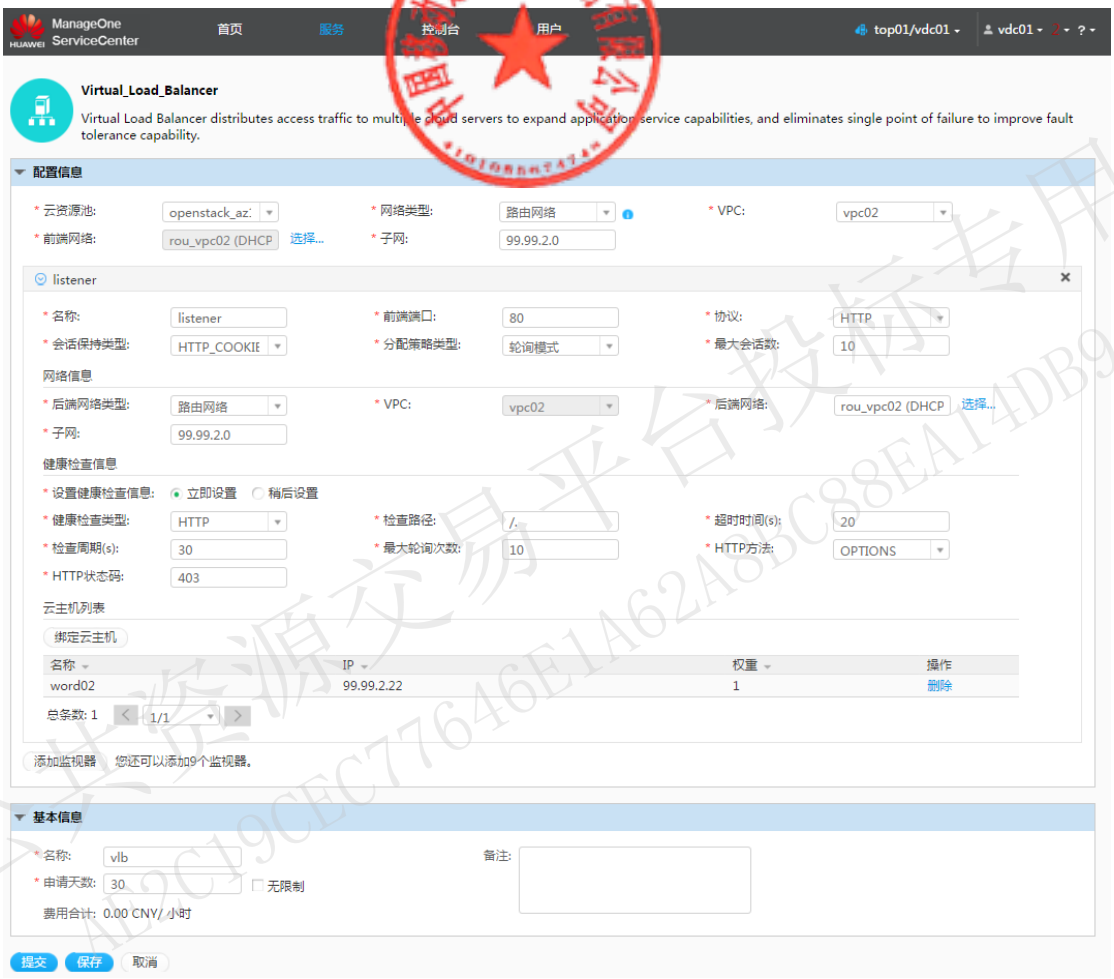
支持监控服务，包括但不限于以下指标：新建连接数、并发连接数、失败连接数、网络入带宽、网络出带宽。

公共资源交易平台招标专用

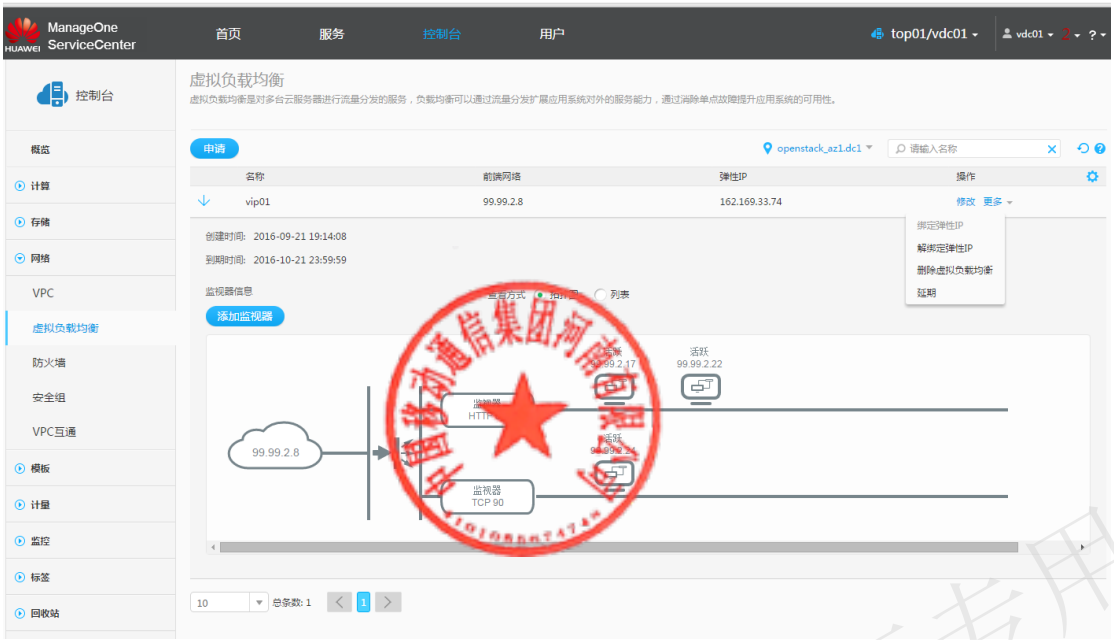
支持 Vxlan 和 Vlan 网络部署。

虚拟负载均衡器服务（简称 VLB）为用户的应用提供负载均衡能力，将访问流量自动分发到多台虚拟机，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。VLB 可以扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

（1）虚拟负载均衡申请



（2）审批后发放



3.2.3.13.3.3.8 多资源池接入管理能力

提供多资源池接入管理能力。支持将多数据中心/资源池的资源进行统一管理和服务发放。

3.2.3.13.3.3.9 资源容量监控

提供对整个数据中心的计算、存储、网络资源容量情况进行监控的能力，支持资源总量、已经分配的资源量、剩余资源量等信息的统计，支持按照资源分区、资源类型等纬度进行统计。



3.2.3.13.3.3.10 统一管理能力

提供统一云运营管理系统，通过数据中心管理系统提供相应的云服务，云服务的服务目录管理设计，云服务资源自动化编排设计，多资源池/多数据中心资源管理设计。

支持多资源池接入。支持将多数据中心/资源池的资源进行统一管理和服务发放；

支持资源集中展现。在资源显示界面中，管理员可以查看各类资源的详情，对资源进行各类操作；

支持对整个数据中心的计算、存储、网络资源容量情况进行监控，支持资源总量、已经分配的资源量、剩余资源量等信息的统计，支持按照资源分区、资源类型等纬度进行统计；

支持灵活定义 SLA 等级如计算性能、存储介质，系统能够按照定义的 SLA 等级根据租户申请的需要在全局调度，分配对应资源。

3.2.3.13.3.3.11 **用户管理能力**

提供用户管理能力，支持用户信息的创建、删除、修改、查询。

访问认证是指基于用户的属性来对用户的真实身份进行鉴别的系统。用户访问认证系统实现各设备及系统用户的集中认证，并为多个系统提供单点登录能力，由认证、授权、访问控制、适配器（代理等）模块构成，认证由统一认证平台完成。

集中的访问认证目标是建立统一、集中的认证和授权系统，授权用户对云服务的使用权，同时防止非授权用户的访问。

关键技术要求包括：

支持用户身份识别与云资源的绑定，并且能够实现：细粒度的访问控制、用户计费、支持遵从，以及数据保护；

用户访问认证应保护云端用户数据的保密性、完整性和可用性；

用户访问认证应包含以下几个方面的功能：强认证、单点登录（SSO）、权限管理、云资源的记录和检测；

支持常用认证方式并提供通用认证接口。

支持支持使用数字证书进行身份认证，支持 CA Key 的物理介质的管理与使用

提供云用户访问日志记录。

支持云用户账户锁定。

应能够根据用户、用户组、用户级别的定义来对资源的访问进行集中授权；

公共资源交易平台技标专用

云用户访问认证管理流程应执行 IT 安全管理定义的策略。

管理职能的访问认证应建立在强认证或基于角色的访问认证机制之上，且强大的运作流程应支持管理权限的生成和撤销；

通过定期审计访问认证和管理员认证，以验证最小特权和职责分离。

3.2.3.13.3.3.12 **业务流服务管理**

支持服务审批待办。管理员可以查看当前所有需要自己审批的服务申请单并进行审批；

支持多级审批，系统默认提供一级审批，系统管理员也可以给服务指定多级审批，并指定每一级审批的角色；

支持服务定义。在服务定义时，管理员可以指定服务的名称、描述、图标等基本信息，同时还可以指定各类服务的参数定义，减少专业参数选择对用户造成的困惑；

配置服务目录管理能力，包括为租户提供服务申请入口，以及用户服务申请、管理员审批能力，以及服务的申请/变更/撤销管理能力。

3.2.3.13.3.3.13 **网页防篡改**

产品形态:产提供B/S架构的产品控制台,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的网页防篡改技术。

防护系统支持：网页防篡改系统应该支持 Windows、linux 等主流操作系统网站防篡改，应支持 IIS、Weblogic、Websphere、Apache、Tomcat 等 Web 服务器。

文件保护：支持对静态和动态等各类网页文件的保护，同时支持防护模式和监控模式两种模式的防篡改模式。

文件同步能力:应支持文件多线程同步,并可以设置文件空闲同步时间周期、发布时间周期等设置。

防护能力：系统可以从本地或异地备份文件夹自动同步到监测目录中，加强文件安全性。需满足等保三级要求，支持主/备目录，主/备服务器备份模式，提供网页防篡改的发布模式，能和主流 CMS 系统集成进行内容发布，提供 32、64 位系统集成。支持大规模连续篡改攻击防护。支持不依赖访问事件的篡改后自动恢复功能，可直接由篡改动作触发恢复机。

公共资源交易平台投标专用

通过网页防篡改系统建设网页防篡改能力，帮助用户实现对静态区域文件和动态区域文件的保护。动态区域文件保护主要是在站点嵌入 web 防攻击模块，通过设定关键字、IP 等操作进行拦截；静态区域文件保护主要是在站点内部通过防篡改模块进行文件实时监控，发现有对网页进行修改，删除等非法操作时，进行保护，并进行报警。通过建设网页防篡改能力，实现多层次、多方位、全智能化的安全防范机制，全面地保护站点的安全，自动监控、自动还原，为站点提供高性能、高可靠的安全保护机制。

为了保障用户的网页安全，网页防篡改系统应该包含以下几个方面：

（1）网页文件保护

通过 web 防攻击模块、防篡改模块（系统内核层的文件驱动），可对动态和静态网页文件进行完美的保护。按照用户配置的进程及路径访问规则，设置网站目录、文件的读写权限，限制文件目录的增、删、改操作行为，确保网页文件不被非法篡改。

（2）网络攻击防护

web 防攻击模块对每个请求进行合法性检测，只允许规则内合法的访问请求，对非法请求或恶意扫描请求，则立即进行屏蔽，防止 SQL 注入式攻击。Web 核心特征库会定期升级，保障其强大的检测能力。

（3）集中管理

通过监控端集中管理多台 Web 服务器，监测多主机实时状态，制定保护规则，接收 Web 服务器的报警和日志信息。控制 Web 服务器的启用、关闭、禁用等状态，并可对 Web 服务器的日志和报警情况做统计分析。

（4）网站安全发布

使用传输模块从监控端的镜像站点直接更新受保护的网站目录，数据通过 SSL 加密传输，杜绝传输过程的被篡改的可能。

（5）网站备份还原

网页防篡改系统支持监控站点数据备份还原功能，可对监控站点目录文件和数据库进行全量或增量备份。用户可以通过启用发布端的自动发布功能，在不停止备份功能的前提下，自动更新网页，发布端会自动将这些内容更新到 Web 服务器上。

公共资源交易平台技标专用

（6）实时报警

对非法篡改行为，系统会自动记录报警日志，并通过手机短信、电子邮件、syslog 等多种方式通知管理员。能对网站攻击做到快速响应，及时应变。

（7）管理员权限分级

可对管理员及监控端分配不同的权限组合。

（8）日志审计

提供管理员行为日志，包括：时间、事件、操作对象、行为、IP 地址等详尽信息，方便区分正常更新过程还是篡改攻击行为；支持保护日志查询审计功能；用户不能进行日志修改、删除操作，确保日志的准确性与完整性。

（9）站点文件保持

防篡改模块集成在 Web 服务器软件中，通过设定各种站点文件访问过滤规则，对多个站点文件或单个站点的文件夹进行保护。

（10）系统信息检测

管理控制端机器能记录所有监控端 Web 服务器的 CPU、内存、硬盘等应用情况，方便管理员根据提供的硬件信息做升级和维护调整。

（11）系统自我保护

网页防篡改系统能够实时地保护自己，不被非法的删除、修改、卸载等，保证了即使服务器被非法入侵，也不能够对网站进行篡改，不能够对网站管理系统进行破坏。

3.2.3.13.3.3.14 **主机安全、主机杀毒**

服务形态：提供云主机安全产品 SAAS 服务，租户通过账户登录后可查看权限范围内的主机情况，制定安全策略。

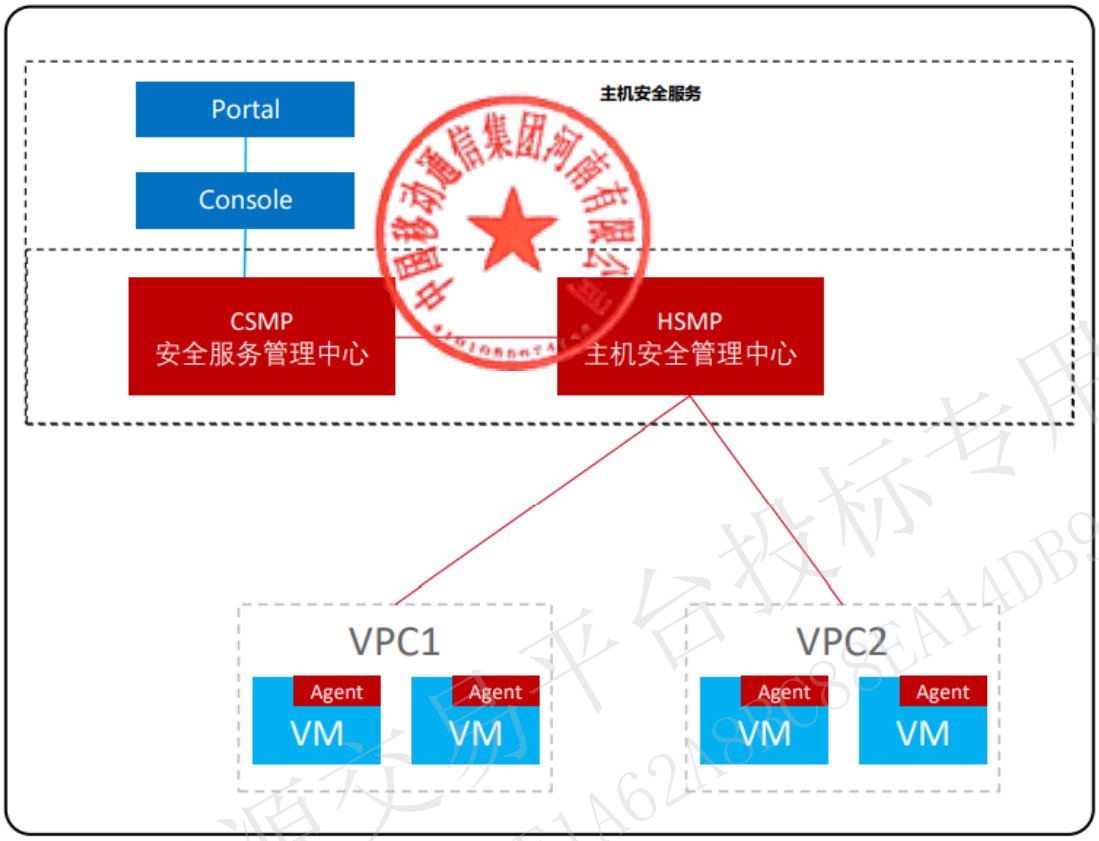
病毒查杀：提供不少于 3 种病毒查杀引擎，可根据不同虚拟化环境和查杀要求灵活开启与关闭；同时产品应支持利用 CPU 虚拟化技术提升系统的安全防护能力。

主动防御：主动防御保护，智能监控系统文件操作行为，利用文件审计关联技术，实时对病毒木马及恶意相关文件进行拦截和防护，特别是针对近期流行的敲诈者木马能够进行有效拦截。

入侵防御：产品应支持入侵防御，可对来自网络层的拒绝服务、缓冲区溢出、

公共资源交易平台投标专用

木马后门、web 攻击、恶意网络扫描、恶意入侵提权等各类威胁流量的检测与防护。入侵防御规则应不少于 11000 条，并支持按照攻击类型进行分组分类，支持对每一类攻击类型单独开启或关闭防护。



3.2.3.13.4 统一运维管理

3.2.3.13.4.1 系统架构

云管平台提供统一的运维能力，解决云数据中心运维的几个核心问题：效率、成本和质量。主要面向专业的运维管理员，如一线驻场工程、云平台运维工程师，运维安全工程师、网络运维工程师以及设备运维工程师等。提供标准化、自动化、智能化的运维能力，方便运维人员及时掌握系统运行状况，并提供故障诊断以及闭环的能力。实现了多云、多数据中心、多资源池、多种云服务的统一管理，提供包含资源管理、集中监控、可视化、运维分析、安装部署等功能模块，支撑日常运维、系统变更、运营分析等运维业务场景。运维对象覆盖基础设施、云服务和应用整个云环境的一体化的运维能力。

云运维具备以下特点：

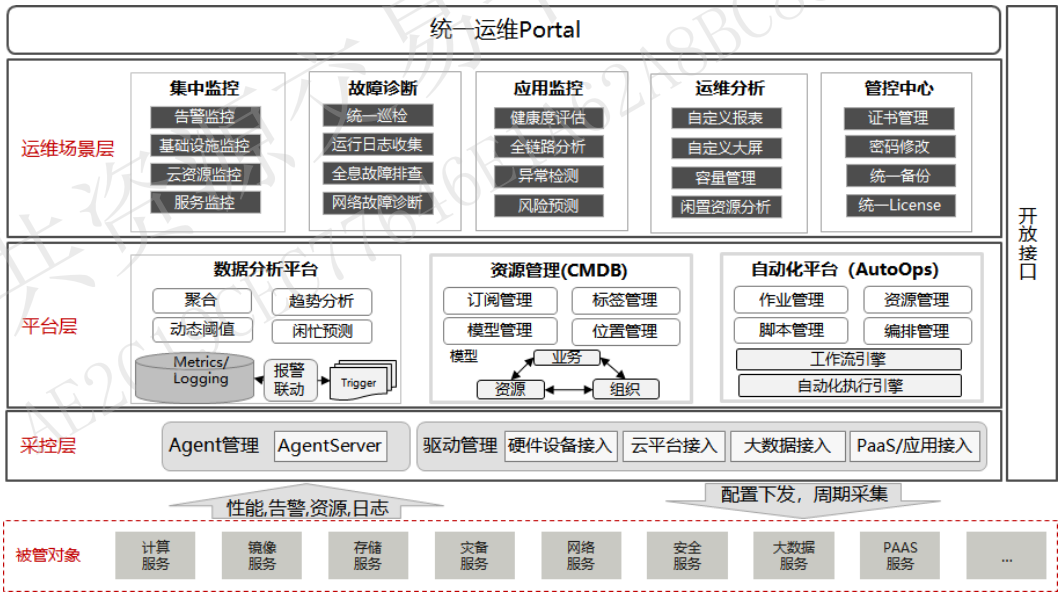
- 架构解耦：云运维架构采用微服务架构，具备良好的敏捷交付和可扩

公共资源交易平台技标专用

展性。

- 能力开放：对外开放北向接口可对接第三方运维平台，第三方可自开发驱动通过南向接口接入集中运维管理平台。
- 分布式架构：每个数据中心部署本地云资源管理系统和物理设备运维系统，负责本地的运维操作、配置和监控数据采集。
- 统一管理：华为云Stack提供了统一的运维门户，和灵活的南向对接能力，基于从南向对接系统中抽取的资源对象的告警、性能、资源等信息，对资源进行监控、统计、分析与预测，从而实现云数据中心资源的统一运维管理。
- 智能分析：利用AI/ML技术，基于客户实际应用场景，构建场景化智能运维能力。

总体架构：作为数据中心运维统一入口，聚焦客户价值，一次登录，一个Portal，提供监、管、控一站式自动化运维平台。



运维服务架构

云运维提供的核心运维能力：

采控层：基于 Agent 和驱动对接技术，实现海量数据插件化的全栈接入能力。

平台层：

- 资源管理（CMDB）：全局统一资源配置管理，管控从基础设施到租

户应用全景资源

- 数据分析平台：构筑大数据平台实现海量数据的存储和分析
- 自动化平台（AutoOps）：改变运维模式，运维动作自动化（脚本，知识）到统一的平台，能力和知识沉淀

运维场景层

- 集中监控：发现问题并预警，提供无盲点，无误报，实时准确的立体化监控能力
- 故障诊断：提升产品可用性，提供全面诊断信息、有效定位手段和故障自愈能力
- 应用监控：改变运维重心，从以资源为中心的监控转变为以应用为核心的监控，持续保障客户业务稳定运行
- 运维分析：降低客户运营成本，提供数据可视，风险可识别，措施可实施的端到端运维能力
- 管控中心：提供统一的配置管理和业务控制中心，降低维护难度，提升运维效率

3.2.3.13.4.2服务能力

（一）资源管理

资源管理（CMDB）是用来存储与管理企业 IT 架构中设备和系统的各种数据信息，依赖相关流程保证数据的准确、及时有效，实现信息共享，提供统一的运维资源配置数据服务，发挥配置信息的价值。

资源管理提供以下主要功能：

资源列表

- 管理员可查看所有物理资源、云资源、云服务、应用及中间件资源，同时提供快速进入对应资源列表查看的入口。
- 管理员可以按照资源池维度、物理位置维度和VDC维度查看资源。
- 资源接入。管理员可以在资源列表中单个或批量录入服务器设备、网络设备或存储设备。

位置管理

公共资源交易平台投标专用

- 通过物理位置管理，用户可以为录入的资源配置物理位置，以便按照物理位置信息查看和维护对应的资源。
- 管理员可查看和管理从对接系统自动同步的资源所在的逻辑位置，方便按照逻辑位置查看和维护对应的资源。

模型管理

- 提供数据中心资源模型管理，提供常用资源模型，并支持模型自定义。
- 资源类型分组管理。CMDB对资源类型进行分组，按照分组层次展示资源类型，可方便查看和管理资源类型。
- 资源类型管理。支持资源类型的增加、删除、修改、查看操作，帮助管理员管理资源类型。对资源类型可以进行属性和资源关系管理，支持对资源属性的增加、修改、删除、查看操作，通过拖拽、可视化编辑等方式提供快捷的属性扩展功能，帮助管理员管理资源属性；支持对资源关系的增加、修改、删除、查看操作，帮助管理员管理资源关系。

标签管理

- 给资源按数据中心、部门、项目和业务系统打标签，支持自定义标签。
- 查看预置标签类型下已创建的标签，可以根据需要增加、删除或修改标签，也可以查看当前标签已关联的资源；当预置标签类型无法满足管理员的需求时，管理员可以根据需要自定义所需的标签类型，并在自定义标签类型下增加、删除或修改标签。同时支持同步运营面标签数据，查看运营面各标签与资源的关联关系。

配置审计

- 预置配置审计规则。系统初始化时会默认预置若干审计规则。系统自动化执行审计规则，找出不合规的资源。资源运维人员需要及时处理不合规的资源项，确保CMDB中数据的准确和完整。
- 自定义配置审计规则。管理员或资源维护人员可以根据自身的需求，创建配置审计规则，通过系统自动化审计出不合规的资源。基

公共资源交易平台投标专用
AE2C15CE27646E1A62A8BC88D1

于审计结果，及时修复不合规的数据，保证CMDB数据的准确性。

变更记录

- 当资源发生了新增、删除、更新等变更时，管理员可在变更记录中查看资源变更的详情，及时了解资源发生变更的时间、操作人等。

（二）自动化平台（autoOps）

为管理员提供作业管理，自定义配置操作参数和执行脚本、管理执行目标以及存储参数文件的平台。构建丰富的运维操作库，如内置批量修改操作系统缺省用户密码、批量为操作系统打补丁的日常操作，标准化各种运维场景。并通过编排管理向管理员提供将运维操作库的单个操作，通过图形化的方式编排组合的能力，更大程度上满足各业务场景的自动化运维操作。可以根据企业的运维诉求按需扩展，最大限度的节约人力成本、降低管理风险、告别枯燥的重复工作。实现操作任务一键执行，提升运维效率和满意度。

自动化运维为管理员提供如下功能：

作业：

- 支持作业管理：支持定义作业，可选择多个设备对象和需要执行的操作名称；支持定义立即、定时单次和周期执行计划。
- 支持作业历史，提供作业执行历史详情查询，可查看作业执行情况。
- 支持运维场景管理，支持根据编排、作业所运维内容进行场景分类。

操作库：

- 支持脚本管理：支持编辑操作集，用户可以定义执行脚本，支持python、Shell等格式。
- 支持编排管理：当需要执行一套流程化的操作时，编排管理支持将操作库的单个操作或编排，通过图形化的方式继续编排组合，形成满足各种业务场景的运维流程。
- 支持的预置场景：内置批量修改linux操作系统密码（python/shell）和批量打linux操作系统补丁(shell)原子操作。

配置：

公共资源交易平台投标专用

- 持文件管理：当需要配置操作及编排的文件参数或调取软件包时，文件管理可作为上传及存储参数、补丁包等文件的管理平台，以便在配置执行操作或编排时选择文件类型的参数。
- 支持资源管理：支持ECS、BMS、物理主机、管理虚拟机远程安装Agent。
- 支持安全策略：可以通过控制策略设定控制时间，暂时禁止执行所有操作和编排，也支持控制时间段内的例外添加；通过扫描敏感命令及时排查高危操作，保证操作执行安全可控。

(三)告警监控

“监控全网告警”场景中包括了设置告警规则、告警监控与处理 2 个任务。

- 设置告警规则

运维管理系统支持告警规则的灵活设置，合适的规则可以显著提高告警监控及处理的效率。

下表中列出了所有支持设置的告警规则。

告警规则	说明
告警屏蔽规则	为减少上报用户不关注的告警，可通过设置屏蔽规则直接屏蔽待产生、不关注的告警。屏蔽后的告警将不在“告警监控”和“当前告警”界面中显示。
告警远程通知规则	由于非工作时间或出差等原因，网络维护人员无法通过当前告警界面查看告警,但又想实时了解告警的产生情况时，可通过邮件或短消息方式将上报的告警发送给网络维护人员，方便其及时了解告警信息并采取相应措施。
告警标识规则	设置该规则后系统将自动给符合规则条件的告警设置状态标识。当用户监控或查询告警时，设置过滤条件可将该类告警过滤掉从而精简告警，提升告警处理效率。如调测场景下产生的告警可通过规则将其标识为“维护态”。
告警转工单规则	设置该规则后系统会将指定的告警转成工单，无需人工干预。 如果您的界面没有告警转工单功能，请忽略该任务。

公共资源交易平台投标专用

告警规则	说明
告警级别重定义规则	为优先保障某区域网络设备或某些关键设备通畅运行，可通过重定义告警级别调整告警级别（例如：可将重点关注的告警设置为高级别），网络维护人员将会对该告警优先处理，从而提供优质网络保障服务。新的告警级别只对重定义后上报符合重定义规则的告警生效。
关键设备规则	通过设置关键设备，将特定设备作为告警源，系统可统计并显示关键设备的告警，便于查看、处理和分析这些告警，保障关键设备运行稳定。
设置告警同步规则	对接系统与本系统断连后导致对接系统侧告警无法上报，两者重新连通后需将告警同步到本系统，便于本系统监控。
相关性规则	相关性规则中定义了告警之间的根源衍生关系，在监控或查看告警时可以将衍生告警过滤掉，只关注要处理的根源告警。 根源告警：产生多条相关告警的源头告警。 衍生告警：根源告警产生的多条相关告警。 说明 相关性规则是通过导入规则文件生效，由于规则文件配置复杂，需要联系华为技术支持工程师配置和提供。
闪断/振荡告警处理规则	通过设置该规则，可以选择将闪断或振荡告警抛弃或者归并到历史告警当中，以减少海量重复告警对运维的干扰。 闪断告警：若告警的产生时间与清除时间的间隔小于指定的时间，则该告警称为闪断告警，该时间段称为闪断周期。 振荡告警：指定时间内，同一对象的同一告警交替产生/恢复的次数大于指定值时，则称该告警为振荡告警。
设置工单系统对接规则	设置要对接的工单系统后，所有工单将转交指定工单系统处理。
设置告警汇聚规则	设置该规则后，告警管理将指定周期内上报的重复告警汇聚到同一个告警下，以减少海量重复告警对运维的干扰。

公共资源交易平台技术专用

告警规则

- 告警监控与处理

根据 3GPP（3rd Generation Partnership Project）协议规定，华为云 Stack 运维管理系统主要提供了告警的确认与清除、指定处理人、调整级别、设为无效、设为维护等功能。

名称	作用	说明
确认	标识告警由谁处理，避免多人同时处理同一告警。	对告警进行确认表示告警即将或已经被处理。告警被确认后，由未确认状态变成已确认状态。 如果要更换告警处理人员，可对该告警进行反确认操作。告警被反确认后，由已确认状态变成未确认状态。
清除	标识告警对应的故障是否恢复。	提供了自动清除和手工清除2种告警清除方式。

表 0-5 告警处理

分类	告警状态	说明
当前告警	包括未确认未清除、已确认未清除、未确认已清除3类告警。	提示现网存在未处理的问题，需要管理员关注并处理。
历史告警	即已确认已清除告警。	用于查看和统计，可以为网络性能优化提供数据来源。

告警状态

本特性包含以下功能。

- 告警导出支持“导出选中”和“全部”的告警。
- 支持设置过滤条件或通过资源分组树来监视符合条件的告警。
- 常用的过滤条件有“告警名称”、“告警源”、 “级别”、“告警状态”、“最近发生时间”和“清除时间”等过滤项，选择过滤条件之

后，可以将当前过滤条件保存为过滤模板。也可以通过“选择过滤模板”使用已保存的过滤条件。

- 提供多种获取告警/事件信息的手段，运维人员可选择关心的维度进行告警/事件监控。
- 以告警维护场景为中心，集中提供告警分析处理所需要的信息，减少用户操作，方便用户获取必要信息。

告警参数说明，如下表所示：

参数	参数详细说明
告警ID	告警 ID，用于标识不同种类的告警。
告警流水号	一条告警从产生开始，中间可能经过多次改变，例如级别变更、被清除等，根据该流水号可以唯一的确定一条告警。 告警归并时，原有的告警放入历史告警，当前告警中记录新的告警及新的告警流水号。
列表流水号	告警在归并处理后被赋予的流水号，区别于“告警流水号”。
告警匹配的规则名	告警经过规则匹配后，打上生效的规则标记。
VDC ID	告警源所对应的VDC的ID，与VDC名称一一对应。
VDC名称	告警源所对应的VDC的名称。
次数	记录同一故障点发生同一告警的重复次数或被归并次数，以提高用户的关注和处理效率。 该参数不在“被屏蔽告警”和“历史告警”中显示。
告警源	产生告警的设备/网元。 例如:OSS,即运营支撑系统(Operations Support System)。
名称	告警的名称。根据告警名称可以了解告警源发生了什么故障。如：CPU占用率过高告警，根据名称即可知道是CPU发生了告警。
级别	包括4种级别：紧急、重要、次要、提示。
确认状态	告警的确认状态，两种状态： 已确认：被确认的告警，“确认状态”显示为“已确认”。

参数	参数详细说明
	未确认：被反确认的告警，“确认状态”显示为“未确认”。 该参数不在“被屏蔽告警”中显示。
清除状态	告警的清除状态，有两种状态： 已清除。 未清除。 该参数不在“被屏蔽告警”中显示。
可能原因	描述引起该告警的所有可能原因，引导维护人员处理告警。
振荡次数	振荡期间告警被屏蔽或丢弃的次数。 该参数不在“被屏蔽告警”中显示。
维护状态	告警的维护状态，如“普通”表示告警源正常运行，没有处于调测或升级等状态。 该参数不在“被屏蔽告警”中显示。
确认时间	告警确认的时间。 该参数不在“被屏蔽告警”中显示。
清除时间	告警清除的时间。 该参数不在“被屏蔽告警”中显示。
来源系统	告警来源系统的名称。 说明 两级运维场景下，总部ManageOne运维面展示全网所有的告警，来源系统用于识别当前告警来源于总部还是分部。
来源系统流水号	告警管理为来源系统分配的标识。
告警源类型	发生告警的网元类型。
类型	告警的类型。
操作	提供可对本条告警执行的操作： 确认告警； 清除告警； 核对； 发送邮件通知；

公共资源交易平台投标专用

参数	参数详细说明
	发送短信通知； 设置屏蔽规则； 设置标识规则； 设置远程通知规则； 设置级别和类型重定义规则； 设置名称重定义规则； 设置闪断/振荡规则； 设置汇聚规则。
定位信息	辅助进行故障定位的信息。通过定位信息可以快速地定位到产生告警的位置。
发生时间	如果该告警是归并告警，则发生时间是该告警第一次发生的时间。如果该告警不是归并告警，界面上显示的是该告警的发生时间。 该参数不在“被屏蔽告警”和“历史告警”中显示。
到达网管时间	告警到达告警管理系统的时间。
最近发生时间	如果该告警是归并告警，则最近发生时间是该告警最近一次发生的时间。如果该告警不是归并告警，界面上显示的是该告警的发生时间。 该参数在“被屏蔽告警”和“历史告警”中显示为“发生时间”。
确认用户	执行告警确认操作的用户。若用户进行反确认操作，则会显示反确认用户。 该参数不在“被屏蔽告警”中显示。
清除用户	清除告警的用户。 该参数不在“被屏蔽告警”中显示。
处理人	运维人员可将告警指派给具体用户处理，该字段记录当前处理的用户名。 设置：选中一条或多条告警，单击“指定处理人”，在下拉

公共资源交易平台投标专用

参数	参数详细说明
	菜单中选择操作。 该参数不在“被屏蔽告警”中显示。
可自动清除	告警是否可以自动清除。 是：表示该告警可以自动清除，则产生该告警的故障消除后，该告警的“清除状态”会自动变为“已清除”。 否：表示该告警不可以自动清除，则产生该告警的故障消除后，需要手工清除告警。 该参数不在“被屏蔽告警”中显示。
部署区域	设备部署区域标识。区域可能对应于一个物理的数据中心，也可能对应于逻辑区域。
厂商	网元所属的厂商。
领域	告警网元所属的产品类型。 说明 两级运维场景下，如果是总部上报的告警，则为空，如果是非总部上报的告警，则显示“省级告警”。
IP 地址/URL/域名	告警物理设备的IP地址。
对象类型	产生告警的资源对象的类型，例如单板、文件目录和端口等。
附加信息	记录告警的一些和定位无关的信息，辅助用户理解该告警。
租户标识	告警源所属的租户标识。
租户名称	告警源所属的租户名称。
备注	由用户填写的告警备注信息，长度不超过512个字符。 设置方法：用户可选中一条告警并单击“备注”按钮，输入告警备注信息。
影响业务名称	告警所影响的业务名称。
影响业务标识	是：对业务有影响。 否：对业务无影响。

公共资源交易平台投标专用

参数	参数详细说明
	未知：对业务的影响不明确。
来源系统类型	告警来源系统的类型。
NFV资源池	告警源所属NFV资源池的名称。
备份状态	反映该告警对业务的影响程度，包括3种状态： 是，表示承载的业务已倒换到备用资源上，并没有对现有业务能力造成直接的影响； 否，表示承载的业务未倒换到备用资源上，对于同一个告警，备份状态为“否”对业务的影响程度比备份状态为“是”的告警要高； 未知：表示对于承载的业务是否倒换到备用资源上不能确定。
原因标识	导致该告警的具体原因的ID。
数据中心	告警源所属数据中心的名称。
区域	告警源所属逻辑位置的名称。
清除类型	空：未清除； 正常清除：设备故障恢复，接收到清除告警，告警被自动清除； 复位清除：设备在重启动后，重新开始检测是否存在故障，原来存在的故障告警被自动清除； 手动清除：告警被用户手动清除； 配置清除：资源对象删除使此资源对象相关的告警被自动清除； 相关性清除：告警管理在进行相关性规则处理时，当接收到未清除的衍生告警的根源告警时，则在上报根源告警的同时，自动清除该衍生告警，该衍生告警的清除类型为相关性清除； 系统清除：由于存储空间的容量限制，根据满处理规则对较早上报的告警执行清除；

公共资源交易平台 投标专用
AE2C19...E27764611A62A8BC88EA14DB9

参数	参数详细说明
	状态切换清除：由于设备发生状态切换，设备前一状态的活动告警被自动清除，而后以切换后的设备状态重新上报告警，前一设备状态的活动告警的清除类型为状态切换清除； 网管同步清除：当同步告警时，如果告警管理上原有的未清除告警在同步上来的告警中不存在了，则该告警被自动清除。 该参数不在“被屏蔽告警”中显示。
可用区	告警源所属可用区的名称。
失效状态	缺省为“有效”，在“标识规则”中可将告警设置为“无效”。 该参数不在“被屏蔽告警”中显示。
持续时间	告警“最近发生时间”到“清除时间”之间的时间。 该参数不在“被屏蔽告警”中显示。
资源名称	告警源的资源名称。
资源标识	告警源的资源ID。
阈值信息	包含故障相关的测量指标的门限和当前值。例如：上报“环境温度越限告警”时，需要说明温度过高还是过低，对应的门限值和当前的温度值。

告警参数

ManageOne 支持查看历史告警，历史告警和被屏蔽告警默认按照“告警流水号”排序。。

- 支持告警列表导出。
- 支持历史告警备注。
- 支持设置过滤条件或通过资源分组来监视符合条件的告警。

过滤项	过滤内容
告警名称	告警名称、告警名称组。
告警源	产生告警的设备/网元。
级别	紧急、重要、次要、提示和以上全部。
告警状态	维护态、正常态；有效告警、无效告警。

公共资源交易平台技标专用

过滤项	过滤内容
发生时间	告警发生的时间。
高级设置	告警类型、维护状态、备注、定位信息、告警源、告警流水号等。

告警过滤

ManageOne 支持根据规则屏蔽特定告警。

可设置的屏蔽规则包括告警源（产生告警的设备）、告警名称、屏蔽规则有效时段等。根据规则屏蔽，用户不关注的告警将不在“当前告警”中显示。新增、修改、删除或启停规则会在 1~2 分钟后生效。

告警屏蔽具体包括以下功能：

- 支持按指定具体的告警对象实例设置告警屏蔽规则。
- 支持按指定告警对象范围（比如来源系统、租户等多个维度）设置告警屏蔽规则。
- 支持指定告警级别设置告警屏蔽规则。
- 支持指定具体告警类型ID设置告警屏蔽规则。
- 支持按如上组合条件设置告警屏蔽规则。
- 支持指定屏蔽规则生效的时间范围。
- 支持记录告警被屏蔽的规则名称。

ManageOne 支持事件查看。支持设置过滤条件或通过资源分组树来监视符合条件的事件，事件一般用来表达一些重要的维护操作。例如：卸载开始，系统正常的运行信息。

- 支持事件列表导出。
- 支持设置过滤条件或通过资源分组树来监视符合条件的事件。

过滤项	过滤内容
事件名称	事件名称、事件名称组。
事件源	指定的事件源，可按资源类型和区域进行筛选。
级别	紧急、重要、次要、提示。
发生时间	告警发生的时间。
高级设置	告警类型、维护状态、备注、定位信息、事件源、告警流水号

公共资源交易平台投标专用

过滤项	过滤内容
	等。

告警条件设置

支持将多条同源告警合并成一条告警呈现，支持按照告警闪断振荡规则进行告警抑制：

- 支持将多条同源告警合并成一条告警呈现。即多条相同告警汇聚合并成一条告警呈现，并且在归并后的告警信息中提供告警的首次发生时间、最后发生时间、发生次数等信息。
- 支持按照告警闪断振荡规则进行告警抑制。通过设置该规则，可以选择将闪断或振荡告警抛弃，以减少海量重复告警对运维的干扰。

功能	描述
闪断分析	制定闪断策略，设置闪断周期和执行动作“抛弃”或“屏蔽”。当满足闪断策略时，告警则按照指定动作进行告警处理。屏蔽的告警显示在“被屏蔽告警”中。
震荡分析	制定震荡策略，设置震荡周期，震荡次数和执行动作“抛弃”或“屏蔽”。 当满足震荡策略时，告警则按照指定动作进行告警处理。屏蔽的告警显示在“被屏蔽告警”中。

告警归并

功能	描述
汇聚策略	制定汇聚策略，设置汇聚对象、触发条件、结束条件和汇聚动作。 如XX网元，在20分钟周期内，产生告警数大于2条，将生产一条紧急级别的告警。

告警抑制

ManageOne 支持根据用户设置的标识规则，自动将告警设置为维护态告警或无效告警。当用户监控或查询告警时，设置过滤条件可将该类告警过滤掉从而精简告警，提升告警处理效率。新增、修改、删除或启停规则会在 1~2 分钟后生效。

功能	描述
创建标识规	设置规则名称、条件和动作等内容，创建标识规则。

功能	描述
则	
启用/停用规则	对于暂时不需要使用的规则，用户可在规则列表中选中后，单击“停用”。若要重新使用已停用的规则，可在选中规则后单击“启用”。
删除规则	对于冗余的规则，用户可在规则列表中选中后，单击“删除”，以减少规则的维护工作量。

告警标识

ManageOne 根据用户设置的远程通知规则自动发送告警远程通知，通知形式包括邮件、短信。

- 支持设置通知用户组，当收到符合规则告警后，系统通过邮件、短信方式，通知用户组。
- 支持设置告警清除发送告警通知。
- 支持定义告警通知内容模板。
- 支持按指定具体的告警对象实例设置告警通知规则。
- 支持按指定告警对象范围（比如来源系统、租户等多个维度）设置告警通知规则。
- 支持指定告警级别设置告警通知规则。
- 支持指定具体告警类型ID设置告警通知规则。
- 支持按如上组合条件设置告警通知规则。

ManageOne 支持用户对告警级别、告警类型和告警名称进行重定义，通过设置告警级别和类型重定义规则、告警名称重定义规则，对指定条件的告警进行自动调整，以满足运维管理的要求。

- 支持按设置的规则，当收到符合规则告警后，自动按预置的告警级别进行告警
- 支持按设置的规则，当收到符合规则告警后，自动按预置的告警类型进行告警
- 支持按设置的规则，当收到符合规则告警后，自动按预置的告警名称进行告警

公共资源交易平台投标专用

- 支持为选定的活动告警手工设置告警级别。

ManageOne 支持告警自动确认，即是将处于清除状态的当前告警，按照指定的规则进行自动确认后移入到历史告警列表中。其包括实时、延时确认 2 种，实时确认请选择规则后点击“启用”；延时确认需先进行延时设置，再选择规则后单击“启用”。

运维人员处理告警后，及时将处理经验记录在维护经验库中，以便为后续或他人的维护工作中提供参考和借鉴。“修复建议及维护经验”中管理的维护经验与告警详情中的维护经验为同一个经验库。

- 支持新建告警维护经验。
- 支持告警维护经验的导出和导入。
- 支持TOP N告警展示。
- 告警维护经验支持导入和导出，文件格式是XLS，导入文件大小不能超过2M。最多导入10000条维护经验，若导入的维护经验已存在（根据标识+分组标识判断），则在原有的维护经验后面追加。此时，若原有的维护经验包含了导入后的经验，则不会追加导入后的经验。

（四）基础设施监控

ManageOne 支持对云平台的各类基础设施资源进行监控，提取各类基础设施资源的监控指标，并支持设定阈值产生相应的阈值告警。

测量对象类别	指标名称
物理资源	服务器
	网络设备
	存储设备
资源池	IaaS资源池
	大数据资源池

基础设施监控

下面分别对上述监控对象支持的监控指标和能力进行说明。

【服务器监控】

- 支持设备的位置管理。
- 支持物理服务器硬件性能、告警监控。

公共资源交易平台投标专用
AE2C19CEC7[illegible]62A8B[illegible]

- 支持各厂商主流服务器的告警和性能集中管理。
- 支持服务器SNMP上报告警。
- 支持周期从服务器器件获取数据并进行统计分析。
- 支持设置性能阈值告警，当指标超过阈值时，系统会上报告警。

【网络设备监控】

- 支持设备的位置管理。
- 支持网络设备硬件性能、告警监控。
- 支持各厂商主流网络设备的告警和性能集中管理。
- 支持网络设备SNMP上报告警。
- 支持周期从设备采集各类性能。指标并进行统计分析。
- 支持设置性能阈值告警，当指标超过阈值时，系统会上报告警。

【存储设备监控】

- 支持设备的位置管理。
- 支持存储设备硬件性能、告警监控。
- 支持各厂商主流存储设备的告警和性能集中管理。
- 支持存储设备SNMP上报告警。
- 支持周期从设备采集各类性能指标并进行统计分析。
- 支持设置性能阈值告警，当指标超过阈值时，系统会上报告警。

【IaaS 资源池监控】

- 支持按Region/资源池/AZ/Cluster/主机/虚拟机等多个层次对计算、存储和网络资源池进行监控，结合关键性能指标，持续评估资源池的负载情况，并给出导致负载高的跟因，对和容量进行容量评估，以指导管理员进行容量规划，扩容等，最终达到提高资源利用率的目的。
- 支持Region/资源池/AZ/Cluster的资源、容量、负载监控。
- 同时，系统还提供主机、虚拟机/弹性云服务更细粒度的监控

【虚拟网元监控】

支持网元集群、节点的 360 监控，监控内容包括资源详情、告警、性能、拓扑关系等，支持集群之间、节点之间的性能数据对比分析、支持性能数据的实时刷新。

公共资源交易平台投标专用

- 支持CVS集群，节点监控
- 支持Nginx集群，节点监控
- 支持BR集群，节点监控
- 支持BMSGW集群，节点监控
- 支持ENAT集群，节点监控
- 支持NATGW集群，节点监控
- 支持vRouter集群，节点监控

（五）云资源监控

ManageOne 支持对云平台的各类云资源进行监控，提取各类云资源的监控指标，并支持设定阈值产生相应的阈值告警。

ManageOne 支持对云平台的对发放给租户的弹性云服务器、裸金属服务、云硬盘、VPC 等进行监控

下面是支持的关键云资源实例：

【弹性云服务器实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过弹性云服务器实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【裸金属服务实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过裸金属实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【镜像实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过镜像实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【云硬盘实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过云硬盘实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【对象存储实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过对象存储实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实

公共资源交易平台投标专用

例。

【VPC 云服务实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过虚拟私有云实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

支持 VPC 云服务实例状态和对应 EIP 上行/下行带宽性能监控，支持展示 VPC 内子网、虚拟机、镜像、物理机拓扑关系。

【EIP 云服务实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过弹性 IP 实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【ELB 云服务实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过弹性负载均衡实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【VPN 云服务实例监控】

当运维管理员希望按照云服务类型对资源进行监控，可以通过虚拟专用网络实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【VFW 云服务实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过虚拟防火墙实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【数据库云服务实例监控】

当管理员希望按照云服务类型对资源进行监控，可以通过数据库实例进行监控。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

【安全实例监控】

ManageOne 支持安全类云服务实例状态监控。支持数据库安全服务、Web 应用防火墙、漏洞扫描服务、密钥管理服务、云堡垒机服务、综合日志审计服务、

公共资源交易平台投标专用

数据库审计服务、安全态势感知服务、安全密码机服务。

【推理服务实例监控】

ManageOne 支持推理服务实例状态监控。从资源池、虚拟数据中心以及时间等维度对推理服务任务资源的性能进行统计和趋势分析。

【高阶云服务实例监控】

ManageOne 支持高阶云服务实例状态监控。

当管理员希望按照云服务类型对资源进行监控，可以通过资源监控>租户资源>云资源查看响应高阶云服务实例列表。运维平台提供云服务实例查询和过滤功能，帮助管理员快速找到云服务实例。

（六）服务监控

对 ManageOne 系统服务以及云服务运行时的微服务实例、部署节点、容器集群等资源的性能指标进行实时监控，记录服务运行时所依赖的各类资源的关键性能指标的变化趋势，提示服务运行时的告警信息，通过对服务、部署节点、微服务实例、容器集群等不同维度的监控呈现出所监控服务运行节点和进程的详细监控数据，帮助管理员及时预防潜在的服务运服务行风险。

- 云服务：可独立销售的服务。ManageOne自身也被视作为一个云服务。
- 服务：基于打包、部署、升级等运维管理考虑的功能内聚的一组微服务或组件。
- 微服务：可独立开发部署、粒度较小、采用轻量级通讯机制、松耦合高内聚的软件架构构建单元。
- 微服务实例：服务的最小运行对象，是服务在部署节点上部署的实例，通常对应一个应用进程，ManageOne提供对微服务实例的状态监控，以及微服务实例相关的业务指标的监控能力 。
- 部署节点：服务所部署的节点，网络服务器上划出的具有一定磁盘空间且具有唯一IP的主机或者虚拟机，ManageOne提供对云服务部署节点OS指标的监控能力。
- 容器：ManageOne提供针对华为云CDK和CCE云服务所发放的容器的监控能力。

公共资源交易平台招标专用

功能	描述
监控视图	支持按服务、微服务、微服务实例层级展示云服务相关的监控指标。
微服务实例指标监控	支持监控微服务实例的业务指标、OS指标和容器指标。 业务指标包含各云服务自定义的影响自身业务优劣的监控指标。 OS指标包含云服务部署节点的OS监控指标。 容器指标特指容器化部署的云服务自身的容器指标。
微服务指标监控	支持监控微服务的容器指标和OS指标。 微服务的OS指标为微服务关联的所有部署节点的OS指标聚合的结果，可选三种聚合方式：平均值（avg）、最大值（max）、最小值（min）。 微服务的容器指标为微服务关联的所有容器指标聚合的结果，可选三种聚合方式：平均值（avg）、最大值（max）、最小值（min）。
服务指标监控	支持监控服务的OS指标。 服务的OS指标为服务关联的所有部署节点的OS指标聚合的结果，可选三种聚合方式：平均值（avg）、最大值（max）、最小值（min）。 支持监控OBS服务的日志类指标。 OBS服务日志类指标特指对OBS服务的业务日志进行格式化和过滤并最终计算出的业务指标，包括租户、桶、集群、主机、容量等多个统计维度。

云服务监控

（七）拓扑管理

通过 eSight 自动发现数据中心内网络设备之间的网络链路，自动生成物理设备之间的网络拓扑视图，建立物理拓扑到虚拟网络拓扑的关联。叠加关键的运维指标如告警数据。支持拓扑编辑，辅助完善拓扑视图。

全自动发现和生成虚拟网络拓扑，自动呈现从虚拟机到物理网络设备之间的

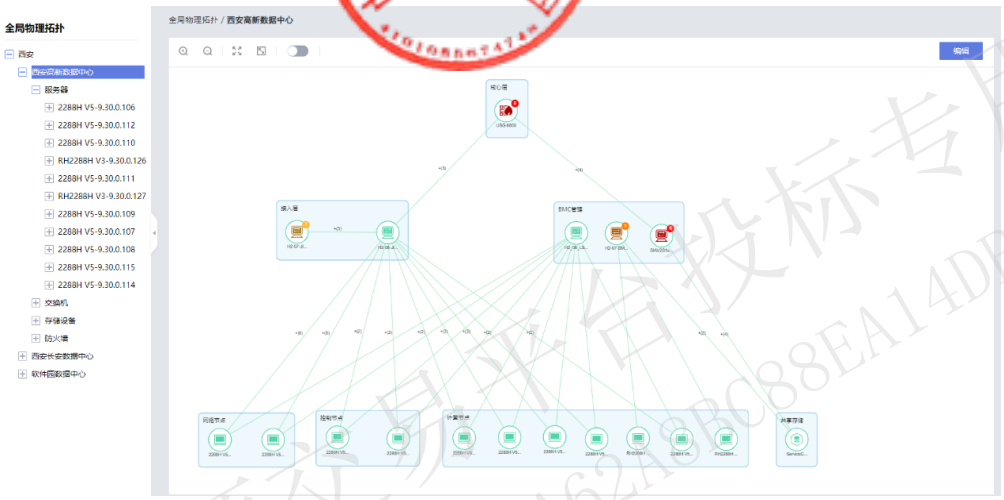
公共资源交易平台投标专用

链路关系。叠加关键的运维指标如告警数据。

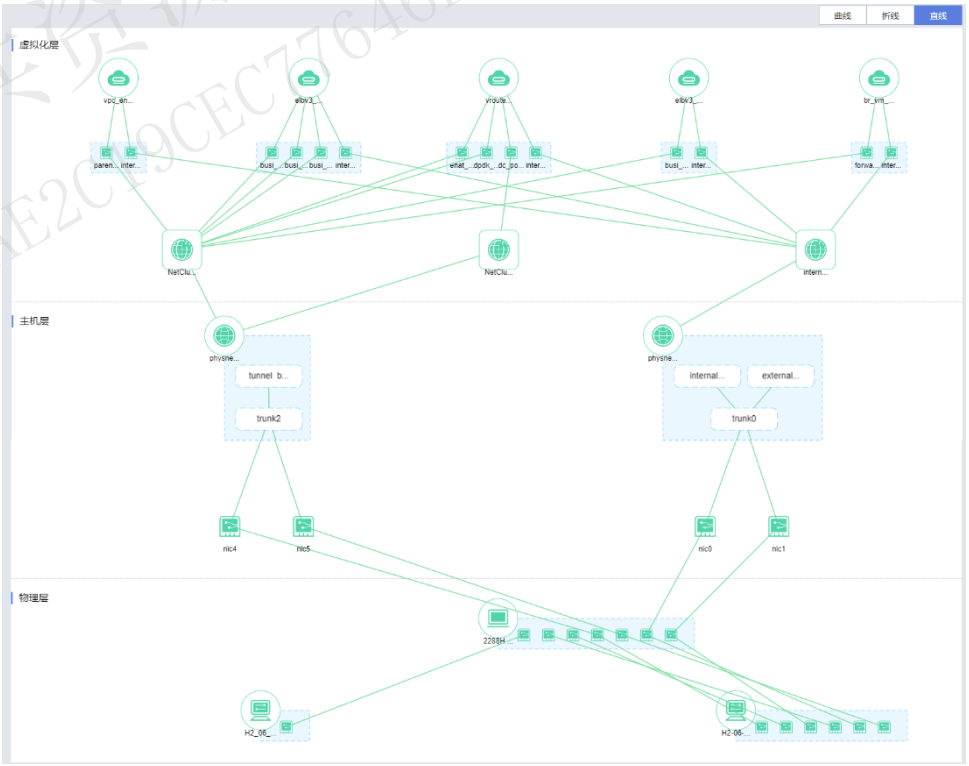
ManageOne 提供全局的拓扑管理，主要支持如下功能：

物理网络拓扑：自动发现物理设备间的网络链路，全自动绘制物理网络拓扑视图，细化到端口级别的网络链路呈现，自动关联设备的告警和性能指标数据，建立网络网络拓扑到虚拟网络拓扑之间的关联，支撑快速进行故障定界分析。支持拓扑视图自定义编辑，满足个性化诉求。

虚拟网络拓扑：全自动发现和生成虚拟网络拓扑，自动呈现从虚拟机到物理网络设备之间的链路关系。叠加关键的运维指标如告警数据等。



物理拓扑管理



公共资源交易中心投标专用
AE2C9CEC77646E162A5BC88EA14DB9

（八）URL 拨测

支持运维管理员配置针对客户的业务系统，以 URL、PING 等协议形式，实施定期的可用性、可连通性的定期拨测，实现对重点关注业务、对象的主动运维，及时发现可用性风险。

Manageone 提供 URL 拨测的能力，分为租户面与管理面的拨测能力：

- 租户面的URL拨测能力

被探测目标为客户的业务系统/业务节点，位于资源池租户面。当前支持配置 URL 以及 PING 的方式实施拨测，周期实施拨测动作。

- 管理面的URL拨测能力

华为为客户提供的云平台中相关系统位于管理面，其可用性状态直接影响到整个云平台的可用性。当前支持云平台的各系统、各云服务针对自身的业务，配置 URL 拨测任务，以及时发现故障，提升故障定界、定位的效率。

（九）容量管理

ManageOne 提供容量视图，管理员可以了解计算、存储、网络等基础资源的容量信息和容量使用的历史趋势。

- 支持按不同维度查看容量视图。

可根据 Region、资源池、AZ、主机组选择不同内容进行查看。

- 支持展示资源池（计算、存储、网络）的容量使用情况。
  - 计算池展示宿主机状态、弹性云服务器状态、、管理虚拟机状态、CPU分配率和内存分配率等信息。
  - 存储池展示存储资源概览、存储池分配率TOP5、存储池列表等信息。
  - 网络池展示弹性IP和网络资源列表等信息。
- 支持容量使用的历史趋势查询。

查看当前、过去一周、过去一个月、过去三个月的资源容量信息。

- 支持导出当前及历史容量信息，定期对资源容量的使用情况进行分析。

ManageOne 提供云服务（ECS、EVS、EIP）容量阈值设置能力。管理员可根据需要，设置指定 Region 的各项阈值规则，当容量消耗达到指定阈值时，产生容

公共资源交易平台投标专用
AE2C15CE0776461A62A8B688EA14DB9

量风险告警，提醒容量管理员及时发现容量风险。

- 支持默认阈值规则。

系统提供默认的容量阈值告警规则，管理员可根据需要设置容量指标阈值。可设置阈值的容量指标包括 vCPU 分配率、vMemory 分配率、存储使用率、存储分配率、数据存储使用率和弹性 IP 使用率，并可针对不同的告警级别设置阈值。

- 支持自定义阈值规则。

当系统默认的容量阈值告警规则无法满足要求，管理员可根据需要自定义阈值规则，自定义规则可以指定具体的区域、AZ 等作用范围，并可针对不同的告警级别设置阈值。

ManageOne 通过历史容量指标给出容量预测的能力，以便管理员对资源容量做好规划和扩容。

以业务发放视角，提供各个资源池中云服务（ECS、EVS、EIP）容量指标的剩余可发放天数和预计到期时间。

基于历史趋势数据，提供未来半年的容量消耗预测曲线。

（十）运维报表

系统预置设备数量统计报表、资源利用率分析报表、容量统计分析报表、租户资源统计分析报表和告警统计报表，帮助用户快速实现业务分析。

- 支持按15分钟、30分钟、1小时、天、周、月设置报表筛选条件，支持相对时间和绝对时间。
- 支持多维度筛选对象，数据的维度取决于源数据。
- 支持多指标筛选，包括指定报表展示数据大小，默认全量展示；选择指标范围；指标的排序方式，支持降序和升序两种；指标的过滤条件，支持and、or两种过滤条件和">、>=、<、<=、=、不等于"多种条件语法。
- 支持钻取操作，对报表中具有层级关系的维度（例如，区域、资源池、可用分区、多节VDC）进行上钻和下钻操作。
- 支持报表按Excel格式导出。

分类	报表名称	描述
设备数量统计报表	设备数量统计	用于统计区域维度各种设备数量。

公共资源交易平台技标专用

分类	报表名称	描述
业务分析报表	业务资源利用率分析	从逻辑位置、时间等维度对业务资源(弹性云服务器，物理机)的数量及资源利用率的统计和趋势分析。
	应用统计	从应用、类型、区域等维度对应用的健康度和繁忙度进行统计和分析。
资源利用率分析报表类型	弹性云服务器资源利用率汇聚分析	用于统计区域、可用分区、集群维度的弹性云服务器资源使用情况。
	弹性云服务器资源利用率TOPN	用于统计弹性云服务器资源使用TOPN。
	计算资源资源利用率趋势	用于统计区域、可用分区、集群维度的计算资源某段时间的使用趋势。 展示形式包括表格和图表。
	计算资源资源利用率分析	用于统计区域、可用分区、集群维度的计算资源某段时间的平均使用情况。
	物理主机资源利用率TOPN	用于统计系统所有物理主机资源使用情况。
	云平台管理系统资源利用率分析	用于统计各云平台管理系统的资源使用率情况。
	闲置虚拟机资源利用率分析	用于统计最近一段时间CPU使用率最大值小于5%且内存使用率最大值小于10%的虚拟机资源使用情况。
	繁忙虚拟机资源利用率分析	用于统计最近一段时间CPU使用率最大值大于80%且内存使用率最大值大于80%的虚拟机资源使用情况。
容量统计分析报表	块存储资源容量视图（管理域）	用于统计管理域的区域、可用分区维度的块存储资源当前分配和使用情况。 管理域指可用分区的管理属性为“管理”。

公共资源交易云专用章

分类	报表名称	描述
	块存储资源容量视图（非管理域）	用于统计非管理域的区域、可用分区维度的块存储资源当前分配和使用情况。 非管理域指可用分区的管理属性为“非管理”。
	块存储资源容量趋势	用于统计非管理域的区域、可用分区维度的块存储资源一段时间分配和使用趋势。 展示形式包括表格和图表。
	对象存储容量视图	用于统计区域维度的对象存储资源当前分配和使用情况。
	对象存储容量趋势	用于统计区域维度的对象存储资源一段时间分配和使用趋势。 展示形式包括表格和图表。
	计算资源容量视图（管理域）	用于统计管理域的区域、可用分区、集群维度的计算资源当前的分配和使用情况。
	计算资源容量视图（非管理域）	用于统计非管理域的区域、可用分区、集群维度的计算资源当前的分配和使用情况。
	计算资源容量趋势	用于统计非管理域的区域、可用分区、集群维度的计算资源一段时间分配和使用趋势。 展示形式包括表格和图表。
	资源池弹性云服务器数量趋势	用于统计云资源池区域、可用分区、集群维度的弹性云服务器一段时间内的发放数量趋势。 展示形式包括表格和图表。
	资源池弹性云服务器	用于统计云资源池区域、可用分区、集

公共资源交易平台投标专用

分类	报表名称	描述
	数量统计	群维度的弹性云服务器当前时间的发放数量情况。
	资源池云硬盘数量统计	用于统计云资源池区域、可用分区维度的云硬盘一段时间内的发放数量情况。
	资源池云硬盘数量趋势	用于统计云资源池区域、可用分区维度的云硬盘一段时间内的发放数量趋势。 展示形式包括表格和图表。
	弹性IP容量视图	用于统计云资源池区域维度的弹性IP当前时间的使用数量情况。
	弹性IP容量趋势	用于统计云资源池区域维度的弹性IP一段时间内的使用数量趋势。 展示形式包括表格和图表。
租户资源统计分析报表	VDC资源利用率分析	用于统计VDC维度弹性云服务器的资源利用率。
	VDC资源利用率趋势	用于统计VDC维度弹性云服务器一段时间内的资源利用趋势。 展示形式包括表格和图表。
	VDC弹性云服务器资源利用率分布	用于统计VDC维度的弹性云服务器使用和闲置数量分布。
	VDC云资源数量统计	用于统计VDC维度的云资源（ECS、EVS、EIP、VPC）数量。
	VDC新增云资源数量统计	用于统计VDC维度的云资源（ECS、EVS、EIP、VPC）在某段时间的新增数量。
告警统计报表	资源池当前告警数量趋势	用于统计云资源池区域维度的当前告警数量趋势。 展示形式包括表格和图表。
	资源类型当前告警数量趋势	用于统计各资源类型的当前告警数量趋势。

公共资源交易云专用技术专用

分类	报表名称	描述
		展示形式包括表格和图表。
	按区域告警数量统计	用于统计最近一周各资源池区域维度所有告警数量。
	按网元类型告警数量统计	用于统计最近一周各网元类型所有告警数量。
	按告警类型维度统计告警数量TOPN	用于统计最近一周同一告警上报次数TOPN的告警。 告警ID与告警分组ID唯一标识一条告警。
	按网元对象维度统计告警数量TOPN	用于统计最近一周网元上报次数TOPN的告警。

表 0-6 运维报表

分类	报表名称
云资源	弹性云服务器明细、云硬盘明细、裸金属服务器明细、弹性IP明细、弹性负载均衡明细。
物理资源	物理主机明细、服务器明细、网络设备明细、网络设备端口明细、存储设备明细、控制器明细、LUN明细、FC交换机端口明细。
大数据	大数据集群明细、大数据主机明细。
VDC	VDC明细、VDC配额明细。

系统预置明细报表

当管理员通过默认展示的报表不能清晰、直观地获取需要的关键信息时，可以将多个维度和指标进行组合，快速实现分析和计算，获取需要的有效业务数据信息。支持通过选择数据集方式快速自定义报表。如虚拟机性能报表

维度/指标	说明
时间	15分钟、30分钟、60分钟、1天、周、月、年
资源维度	虚拟机名称

公共资源交易平台投标专用

维度/指标	说明
监控指标	示例：CPU平均使用率、内存平均使用率、磁盘平均使用率、磁盘平均IO，支持的指标详情参考6.3.1
监控指标过滤条件	指定报表展示数据大小、指派排序方式和自定义指标条件，如CPU平均使用率>50

维度报表

ManageOne 提供定时生成周期报表的功能。管理员可以配置周期性任务，选择指定的报表和周期任务执行方式，并以邮件方式发送给指定的人员，还可以查看周期性报表任务的状态以及历史周期性报表，了解周期性报表的执行情况。当任务执行成功后，管理员可定时查看生成的报表或定时接收邮件。

- 支持报表输出excel格式和邮件通知设置。
- 提供周期任务管理的功能，支持任务状态查看。

（十一）大屏展示

系统提供数据中心整体维度大屏，展示数据中心资源统计、状态统计以及容量分配趋势。

- ManageOne预置数据中心总览、资源池总览、VDC资源详情、多云资源总览、云驾驶舱总览，展示数据中心资源统计、状态统计以及容量分配趋势。
- ManageOne提供首页的布局设置及内容设置能力，系统管理员可以通过添加自定义大屏、调整大屏显示顺序等方式查看关心的大屏信息。

视图模板	介绍
数据中心总览	提供数据中心关键物理资源统计、状态，并分区域展示云服务业务发放情况。
资源池总览	提供资源池关键虚拟化资产资源统计、状态，并展示虚拟资源的分配率和使用率。
VDC资源详情	按VDC展示资源容量和使用趋势，并提供各类云服务资源统计。
多云资源总览	提供多云资源统计和状态展示。

公共资源交易平台投标专用

视图模板	介绍
云驾驶舱总览	提供数据中心概览、逻辑拓扑和物理拓扑。

表 0-7 大屏详情

运维管理员可以通过自定义可视化部件，将性能、容量、资源等不同维度的数据通过曲线图、饼图、柱状图多种样式组合展示在不同的 Dashboard 中，也支持卡片、地图、文字、表、树、图片等多种方式，帮助管理员监控、演示和汇报。

- Dashboard提供大屏布局设置能力，支持超大画面和不同分辨率展示。
- Dashboard支持创建、编辑、删除、预览、移动分组、收藏至首页、复制功能。
- Dashboard提供丰富的展示控件和灵活强大的拖拽式自定义能力，同时预置大量丰富的参考场景模板。
- Dashboard组件自定义数据集、维度和指标，数据展示灵活编辑。
- Dashboard组件支持自定义样式，定义组件显示的类型、标题、描述、颜色，以及组件堆叠/平铺的方式。
- Dashboard组件支持导入导出功能。
- Dashboard组件支持只读权限的大屏管理员。

3.2.3.13.5 云运维管理系统功能

提供统一云运维管理系统，提供高效的运维管理手段，提升问题处理效率，缩减问题处理时间，在问题发生时可快速自动通知到维护人员，提供分析工具，方便研判故障。提供健康分析功能，能够实时监控并分析数据中心的资源使用状态，评估健康度和风险，协助客户主动运维。提供日常的运维报表，后台运维支持，用户发现问题后应快速分级响应。

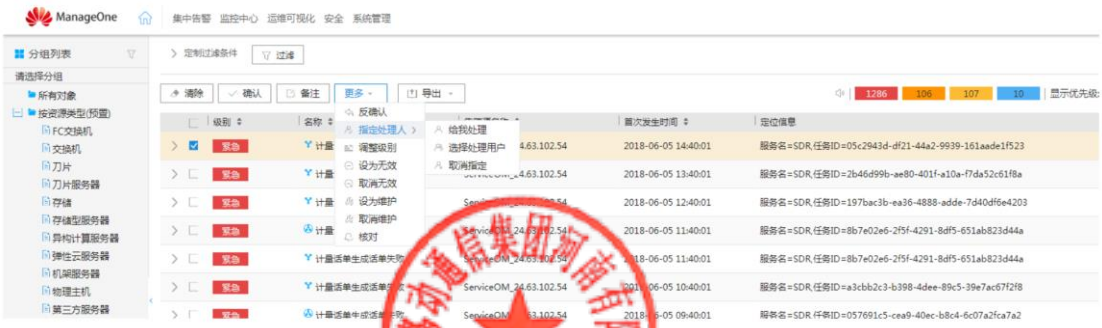
3.2.3.13.5.1 告警及性能管理

（1）支持多维度告警/事件展现。提供按监控对象、按物理位置、按虚拟逻辑、按来源系统、按服务分组等维度查看告警，保证云场景下告警管理的灵活性；

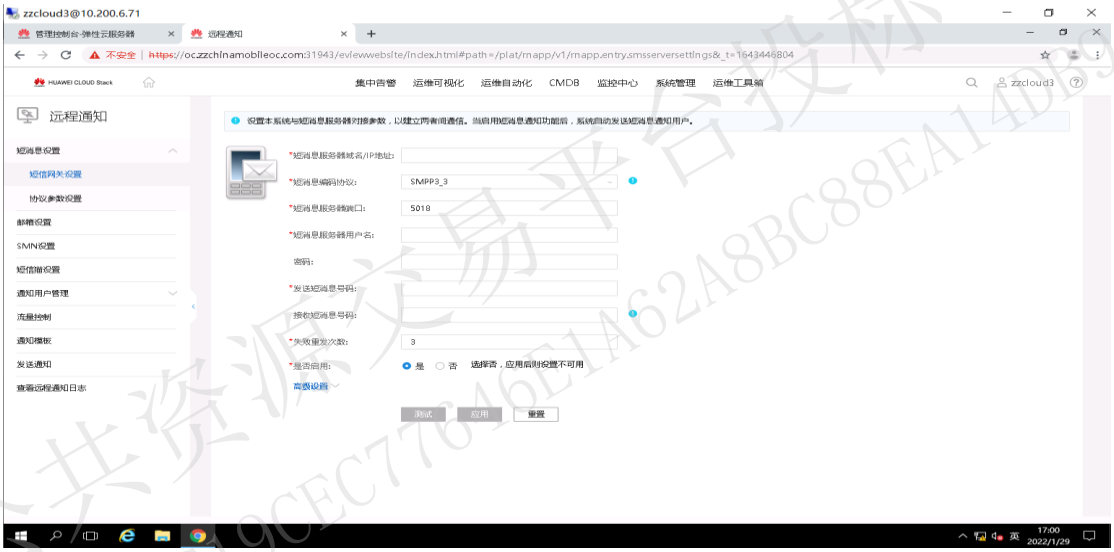
（2）提供告警处理功能，包括确认、清除等，对选择的告警进行处理。支持用户进行告警确认、取消确认、清除告警、更新告警级别、编辑告警备注、编辑

公共资源交易平台投标专用

告警经验关联帮助，协助管理员更好的处理告警事件；



（3）提供告警通知功能。通过设置通知规则，当收到符合条件的告警时，自动通过邮件、短信通知用户。支持按设置的规则，当收到符合规则告警后，通过邮件、短信方式，通知用户，支持逾期升级通知；



（4）支持告警自定义筛选。支持按多个维度的条件组合进行筛选，包括但是不限于按告警名称、状态、级别、来源、告警对象条件等筛选条件，并支持告警导出功能；

（5）支持设置告警级别、以及告警阈值能力，支持设置告警规则，有符合规则的告警，自动按照预置的告警级别进行告警；

（6）支持告警统计报表，可以对已经发生的告警进行分类统计，并输出报表，便于整体的分析数据中心告警事件；

（7）支持搜索查看单个虚拟机信息，支持数据中心、虚拟化平台、集群三个不同粒度查看虚拟机概况，支持按照资源使用率过滤显示。支持把用户查看的性

能指标、设备参数保存成视图，后续查看直接选择视图即可，不需要重新选择参数，提升操作效率。

3.2.3.13.5.2拓扑管理

（1）支持按物理位置查看拓扑，以及整体多数据中心之间的拓扑关系；

（2）拓扑结构支持从资源分配使用的维度查看资源。虚拟化资源是被一个个应用服务使用的，可以从虚拟数据中心，到资源层层展开查看资源的分配使用。

（3）支持拓扑对象操作。可以对拓扑图进行放大，缩小，移动图标，调整布局，并且可以在图中增加或删除虚拟节点；

（4）支持拓扑对象查找。可以输入对象名称或 IP 地址等；

（5）支持大屏展示，可以将仪表盘中的内容展示成大屏模式，方便集中监控；

（6）提供多点信息关联查看及操作的能力。运维人员在查看具体对象信息的同时可以查看与该对象相关的告警、拓扑、时间、性能等多维度信息并且可以进行部分快捷的维护操作。包括选择查看某个对象时可以显示出对象详细信息、告警信息、事件以及性能信息；

（7）支持按物理位置查看拓扑，以及整体多数据中心之间的拓扑关系。



3.2.3.13.5.3报表管理

（1） 支持周期性生成报表，立即生成报表，周期类型包括：天、周、月、季度。只需要设置一次报表参数，即可周期提供报表数据。

（2）支持自动将报表发送到指定的 Email 地址。

公共资源交易平台投标专用
AE2C19CE77646E1A62A8BC88EA1

3.2.3.13.5.4设备管理

（1）统一设备管理：

1）提供统一设备管理能力，统一管理包括数据中心存储、服务器、应用、网络设备（路由器、交换机、防火墙），提供全网资源信息的 Dashboard（分类总数、资源利用情况、关键指标 Top，如 CPU、内存等）；

2）支持管理主机设备、网络设备、存储设备等第三方主流厂商设备的管理；

3）设备规模应满足政务云未来设备增长的要求。

4）设备分组：提供设备分组能力，支持将多台设备划入一个分组，以简化后续对这些设备的批量操作。分组在拓扑中不显示。

（2）服务器管理：

1）基本信息管理：通过机架图等可视化方式，提供服务器以及各部件基本信息、健康状态的展示功能；

2）性能分析：提供网口性能、服务器功耗、CPU 占用率/内存占用率、创建分析任务和时间段性能等多个指标分析；

（3）存储管理

1）提供存储容量利用率预测能力，支持查看和统计存储空间使用情况，包括磁盘空间分配、存储池利用率；支持主机实际存储、虚拟机存储空间使用率查看；提供容量预测的功能，可作为扩容的依据，比如从主机角度预测硬盘容量等；

（4）安全管理

1）用户管理：提供用户创建、删除、查看、修改等功能，缺省提供 admin 用户作为超级用户。其中，用用户密码使用不可逆算法；

2）角色管理：提供角色创建、修改、删除及查看等功能；

3）鉴权管理：提供多种鉴权方式。包括不限于

本地认证：提供用户管理、登录鉴权、安全策略等功能；

LDAP 认证：由 LDAP 服务器对登录请求进行认证；并根据 LDAP 服务器上用户所属用户组，映射到管理系统中所属角色来为用户授权。

（5）网络管理：

1）支持通过流量分析了解流量的构成和分布。根据接收到的 Flow 报文自动添加设备， 并且自动分析设备接口流量，提供各种纬度的报表展现；用户也可

公共资源交易平台投标专用

以灵活调整哪些设备接口监控、哪些不监控；

2）提供接口、应用、来源主机、目的主机、会话、接口组、应用组等多个维度的流量数据；

（6）安全性要求：前后台采用数据传输加密，涉及密码等敏感信息采用加密存储方式，防止泄露。

3.2.3.13.5.5流程管理

流程管理包括：服务台、事件管理、问题管理、变更管理、配置管理、发布管理等。

3.2.3.13.5.6资源监控

（1）资源监控能够支持并提供对计算资源、存储资源、网络资源的性能及运行状 况进行实时监测，并以图形化的形式展示资源状态与利用效率， 提供实时性能数据和历史数据查询、查询支持精确和模糊查询。 对平台主机聚合及计算节点容量全量数据进行实时监控及告警，

（2）能够支持按内存分配率和 CPU 分配率进行筛选、展示。

（3）能够支持数据中心查看虚拟机概况，支持搜索查看单个虚拟机信息。

（4）能够支持物理主机关联设备查询功能。

（5）能够支持自定义日志关键字监控，支持监控节点多节点部署。



3.2.3.13.5.7值班巡检

（1）能够支持并提供物理资源、虚拟资源监测功能，实现管理层面、资 源类别层面的多维度资源监控与管理。

（2）能够支持值班队列管理功能，包括：值班人员管理、值班模式管理、 排

班与交接班管理、值班日历导出、调班申请等。

（3）能够支持巡检统计功能，根据巡检报告总数、成功巡检次数、失败　巡检次数、巡检动态等方面进行统计展示。

巡检报告可推送至相关责任人邮箱。

3.2.3.13.5.8 审计管理

能够支持对堡垒机的登录日志、操作日志、离线日志等审计日志进行展示。

能够支持敏感操作定义功能，并对敏感操作进行展示。

实时展示堡垒机的链接状态，并对超过 2 小时的长链接堡垒机进行单独展示。

3.2.4　政务云安全建设方案

3.2.4.1　安全风险分析

相比于传统计算中心，云计算平台的结构更加一致。同构的设施平台能更好地支持安全管理活动的自动化。同时，安全响应活动也可从一致、同构的云基础设施获益，如容错管理、系统维护。但云服务商通常把云计算平台的安全措施及其状态视为知识产权和商业秘密，客户在缺乏必要的知情权的情况下，难以了解和掌握安全措施的实施情况和运行状态，不能有效监管内部人员对租户数据的非授权访问和使用。

云平台大部分应用都根植在虚拟机环境中，这些应用中包括了很多的对外应用，黑客可直接通过这些应用侵入到虚拟机内部，遗留木马病毒。另外，虚拟机和宿主机本身都有外部的接口，如 USB 接口、虚拟网卡与宿主机物理网卡桥接等方式，使得虚拟机感染外界木马、病毒的风险大大增加。

基于云计算环境的冗余能力、可拓展性可以更好地应对弹性伸缩需求或分布式拒绝服务攻击。然而可用性高意味着需要投入更多的网络和计算资源，这也就暴露了更多的风险面。

备份和恢复策略、规程可能优于用户机构并具备更高的鲁棒性，能够从严重事件中快速恢复。然而当一个资源存在多个副本时，各个副本内容的一致性和剩余信息保护方面难以得到保证。

云解决方案的体系结构扩展到了位于服务端点的云客户端处，为移动办公人

公共资源交易平台投标专用

员带来更高的生产效率。需要注意的是，移动设备需要进行正确的设置和保护，包括限制在其上可以保留的数据类型。

云环境下的数据维护和处理减少了移动工作人员使用便携式计算机、嵌入式设备、移动存储进行传播的风险以及因设备失窃、丢失带来的风险。但如果没有采取足够的安全措施，将面临数据泄漏和被篡改的安全风险。

作为信息化的服务提供者，面对日益增长的业务需求，对网络和系统的稳定性、可靠性、服务质量的要求很高。大量软硬件的投入和增加，也导致了运维管理难度的增大和系统管理人员的工作压力越来越大。

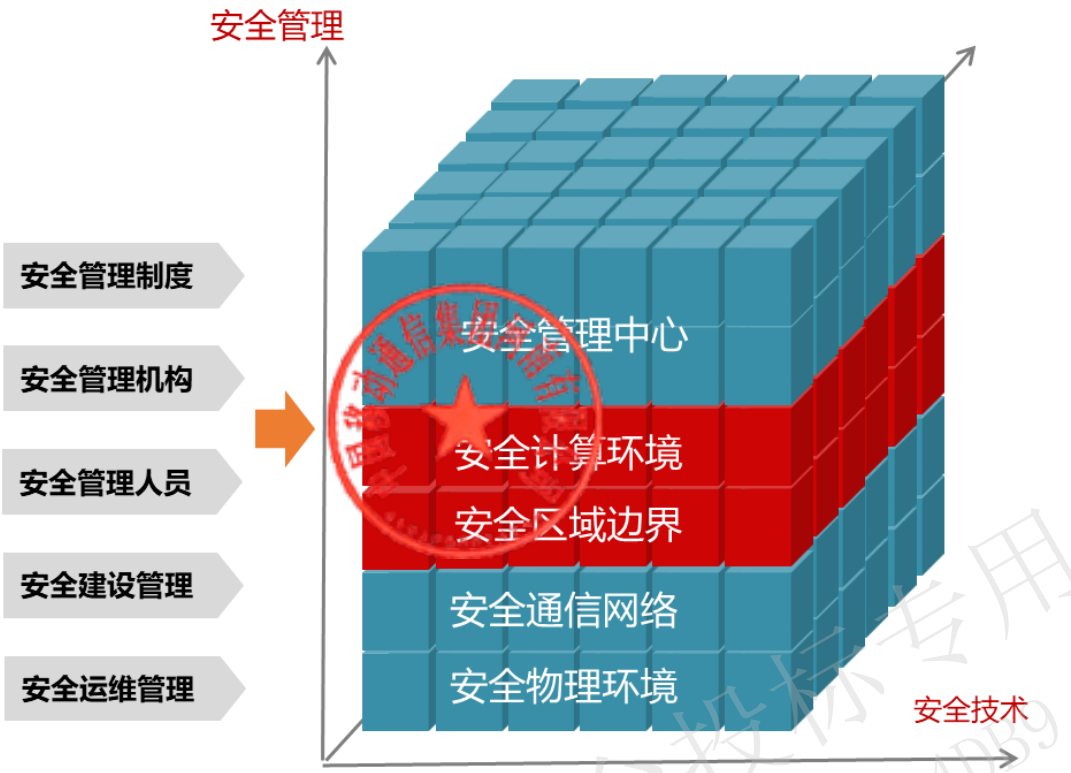
此外，IT 平台系统运维还需要对平台系统的整体运行状况进行有效监控，需要及时发现潜在的问题，这对网络管理工程师又是一个很大的挑战。网管工程师过去经常是在故障发生后，才能去进行处理，工作处于被动状态。有时即使发现了故障，也要花费很长时间去寻找和诊断故障，极大地影响了工作效率。由于没有直观的网络拓扑功能，平台系统的监测和管理显得非常繁琐。如何对各种模块系统进行有效的监测管理，不断提高各种应用的服务质量，是日常安全管理人员急需解决的问题。

3.2.4.2 **云平台安全建设方案**

3.2.4.2.1 安全概述

本次项目的安全保护体系，从安全技术、安全管理以及安全服务三个维度进行设计。根据《网络安全等级保护安全设计技术要求》（GB/T 25070-2019），等级保护三级安全技术从安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面进行构建。

公共资源交易平台投标专用



平台安全保护体系

安全技术体系的建设简单来说就是“一个中心，三重保护”。

“一个中心”指的是安全管理中心，是对信息系统的安全策略及安全机制实施统一管理的平台。按照等保的《基本要求》，第三级（含）以上的信息系统安全保护环境需要设置安全管理中心。

对于整体云数据中心管理平台，我们建议从全局的角度出发，对不同保护等级、不同安全区域的信息系统实施统一的安全管理，即建立全网集中的统一安全管理平台，通过资产管理、脆弱性管理、事件管理、风险管理、策略管理、运维管理、应急管理等手段，实现全网集中的安全监控、风险管理、事件响应。在安全管理平台的基础上，建立安全运营中心，协调信息系统各个环节所采用的安全防护措施和安全管理要素，形成相互关联、高度融合的安全防护平台，实现对安全事件的实时检测、及时响应和综合防护，对网络系统安全防护体系的动态更新，降低安全风险，提升的信息安全监管能力。

“三重保护”指的是按照分域保护的思想，将信息系统从结构上划分为不同的安全区域，各个安全区域内部的网络设备、服务器、终端、应用系统形成单独的计算环境，各个安全区域之间的访问关系形成区域边界，各个安全区域之间的连接链路和网络设备构成了通信网络，因此整体安全保障技术体系将从保护计算

公共资源交易平台公开投标专用

环境、保护区域边界、保护通信网络三个层面分别进行构建，最终形成三重纵深防御的安全体系，并且它们始终都在安全管理中心的统一管控下有序地运行。

保护计算环境：计算环境是对信息系统的信息进行存储、处理的相关部件，包括网络平台、系统平台和业务应用。不同安全等级信息系统的计算环境有着不同级别的保护要求，在进行计算环境保护措施设计时，可以将根据等级保护基本要求、行业安全规范要求和信息系统自身安全风险防护需求，提出各信息系统计算环境内部的安全技术保护措施。

保护区域边界：区域边界是信息系统计算环境与通信网络之间实现连接的相关部件。不同安全等级信息系统的区域边界有着不同级别的保护要求，在进行区域边界保护措施设计时，可以根据等级保护基本要求、行业安全规范要求和信息系统自身安全风险防护需求，对各信息系统区域边界实施安全保护技术措施。

考虑到相邻的信息系统存在区域边界设备共享的情况，如果不同安全级别的信息系统通过同一套安全措施进行边界保护，这个边界保护措施及其所采用的保护策略应满足最高级别信息系统的安全保护要求。

保护通信网络：通信网络是对信息系统计算环境之间进行信息传输的相关部件，包括骨干网/城域网及局域网主干核心系统。不同安全等级的通信网络有着不同级别的保护要求，在进行通信网络保护措施设计时，需要根据等级保护基本要求、行业安全规范要求和信息系统自身安全风险防护需求，实施通信网络安全保护技术措施。

考虑到不同安全级别的信息系统共享同一网络线路和网络设备传输数据的情况，该通信网络的安全保护措施及其所采用的保护策略应满足最高级别信息系统的安全保护要求。

3.2.4.2.2 安全物理环境要求

数据中心已制定并实施完善的物理和环境安全防护策略、规程和措施。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以确保数据中心的物理和环境安全。

机房选址：数据中心机房选址一定程度上决定面临的自然灾害以及可能的环境威胁。数据中心选址一律避开自然灾害不利或危险的地区，减少周边环境对数据中心产生的干扰，如 400 米内无实验室、化工厂等危险区域。同时，选址上保证了数据中心正常运营需要的配套资源，如市电、水、通信线路等。

访问控制：数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置了 7*24 小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关；数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。

安保措施：数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行 7*24 小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。

电力保障：数据中心采用多级保护方案保障业务 7*24 小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源(UPS - Uninterrupted Power Supply)，提供短期备用电力供应。在机房供电线路上配置了稳压器和过压防护设备。在供电设备及线路上还设置冗余或并行的电力电缆线路为计算机系统供电。

温湿度控制：通过精密空调、集中加湿器自动调节，数据中心机房温湿度保持在设备运行所允许的范围内，使设备元器件处于良好运行状态。机柜冷热通道有合理的布置，利用架空地板下空间作为静压箱来给机柜送风，并设置了冷通道密闭，以防止局部热点。

消防能力：数据中心建筑防火等级均按一级设计施工，使用了 A 级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自

动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统，得以控制火情。

例行监控：数据中心的电力、温湿度、消防等环境运行状态通过日常巡检制度得到例行监控，安全隐患能被及时发现并修复，确保设备稳定运行。

供水排水：数据中心的供水和排水系统均有合理规划，保证了总阀门正常可用，确保关键人员知晓阀门位置，以免信息系统受到漏水事故破坏。机房建筑和楼层均有抬高场地，在外围设置了绿化地排水沟，加速排水，以降低场地积水倒灌风险。建筑满足防水一级标准，保证了雨水不能通过屋顶、墙壁向机房渗透。，数据中心也配备了及时排水的设施，供水实时使用。

防静电：数据中心机房铺设了防静电地板，导线连接地板支架与接地网，机器接地以导走静电。在机房大楼顶部设置了避雷带，供电线路安装了多级避雷器，导走电流。

3.2.4.2.3 安全通信网络

（一）结构安全及安全域划分设计

在核心交换、边界安全设备均采用双机冗余，安全域的详细划分请见**错误!未找到引用源。错误!未找到引用源。** 章节。

（二）网络链路负载均衡设计

为了确保云平台核心后台系统网络能提供更高效、合理、可靠的网络链接服务，本方案设计的网络防护系统，满足链路的负载均衡的应用需求。

（三）通信网络数据传输保密性、完整性保护、可信接入保护设计

云平台建设安全接入平台，通过部署 VPN 系统、接入认证管理系统、防火墙系统，对远程部门接入用户提供远程接入和数据加密传输功能，防止数据篡改和数据窃听等风险。

（四）运维安全审计

需要考虑针对运维人员的运维审计系统。审计内容包括运维人员行为、网络设备系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等，并能够根据记录数据进行分析，并生成审计报表，同时具备审计进程保护，避免受到未预期的中断，具备审计记录的保护功能，避免受到未预期的删除、修改或覆盖等

公共资源交易平台投标专用

操作。对于支持租户收集和查看与本租户资源相关的审计信息的功能，则由云平台的安全即服务扩展能力提供。

3.2.4.2.4 安全区域边界

（一）边界结构安全

云平台不同租户之间通过 VRF、VLAN/VXLAN、VPC 方实现不同租户间虚拟网络资源之间的隔离，并在交换机/虚拟交换机上通过配置配额 QoS 避免网络资源过量占用；

对于保证云计算平台管理流量与云服务客户业务流量分离措施方面，华为云安全解决方案的网络平面划分为业务平面、存储平面和管理平面，且三个平面之间是隔离的。保证管理平台操作不影响业务运行，最终用户不破坏基础平台管理。

通过部署华为 eSight 网管系统以及云平台网管模块能够识别、监控虚拟机之间、虚拟机与物理机之间的网络流量。

（二）边界防护及访问控制措施

公网访问逻辑隔离支持访问控制设备和 VPN 功能，例如，防火墙。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；同时系统具备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 等协议的命令级的控制；并在会话处于非活跃一定时间或会话结束后自动终止网络连接，充分确保系统非实时在线层面的安全保护功能。VPN 功能具备对远程拨号访问权限的用户数量进行限制。

云平台承载着多个租户的业务，由于各租户共享着物理资源，因此存在租户资源滥用、数据泄漏、虚拟机之间相互攻击等风险，所以保障租户业务资源相对独立(计算资源、存储资源、网络资源)、数据不被其他租户非法访问、资源可单独管理，是尤为必需和重要的。在网络资源平面，每个租户独享一台虚拟出口防火墙，和分布式虚拟化路由器。每台虚拟防火墙、虚拟路由器的资源是独立的，租户的业务及网络配置不会影响到其他租户，同时管理员也可对租户网络进行单独的配置和管理。

通过部署南北向出口防火墙设备，能够对非授权设备私自联到内部网络的行为及内部网络用户私自联到外部网络的行为进行检查并记录。能根据用户信息、主机信息、IP 信息等准确定出非法互联位置，并对其进行有效的网络阻断控制。

公开资源 云平台投标专用

能在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马攻击、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。

在南北向出口防火墙上配置入侵检测功能，入侵检测系统（Intrusion Detection System）是对防火墙有益的补充，入侵检测系统被认为是防火墙之后的第二道安全闸门，对网络进行检测，提供对内部攻击、外部攻击和误操作的实时监控，提供动态保护大大提高了网络的安全性。

入侵检测系统主要有以下特点：

- 事前警告：入侵检测系统能够在入侵攻击对网络系统造成危害前，及时检测到入侵攻击的发生，并进行报警；
- 事中防御：入侵攻击发生时，入侵检测系统可以通过与防火墙联动、TCP Killer等方式进行报警及动态防御；
- 事后取证：被入侵攻击后，入侵检测系统可以提供详细的攻击信息，便于取证分析。
- 另外，对于网站敏感内容监测，则华为云平台安全扩展能力具备网站敏感内容监测能力。

通过在南北向出口防火墙上配置专用的网络边界防病毒网关设备，对各种恶意代码进行检测和清除，建立起整个系统的网络层面的恶意代码防护措施。系统支持自动及手工方式对恶意代码库的升级和检测系统的更新功能。

针对云平台用户使用网络进行无关操作影响网络效率，以及使用主机搭建无关服务、通过网络传递敏感信息、通过论坛等发表不负责任的言论及其他一些监管者不期望发生的行为等，需要建设相关技术能力对网络资源使用情况及网络行为内容进行还原和记录，以备审计。在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。

根据云平台的要求，收集各自控制部分的审计数据和实现各自控制部分的集中审计；当发生虚拟机迁移或虚拟资源变更时，安全审计机制可应用于新的边界处；为安全审计数据的汇集提供接口，并可供第三方审计。租户自身安全审计则由云平台安全即服务扩展能力提供。

在云平台的互联网出口处，部署两台 Anti-DDoS 设备，两台设备工作在集群模式。边界路由交换设备通过策略路由将待清洗流量牵引至 DDoS 清洗设备，设

公共资源交易平台技标专用

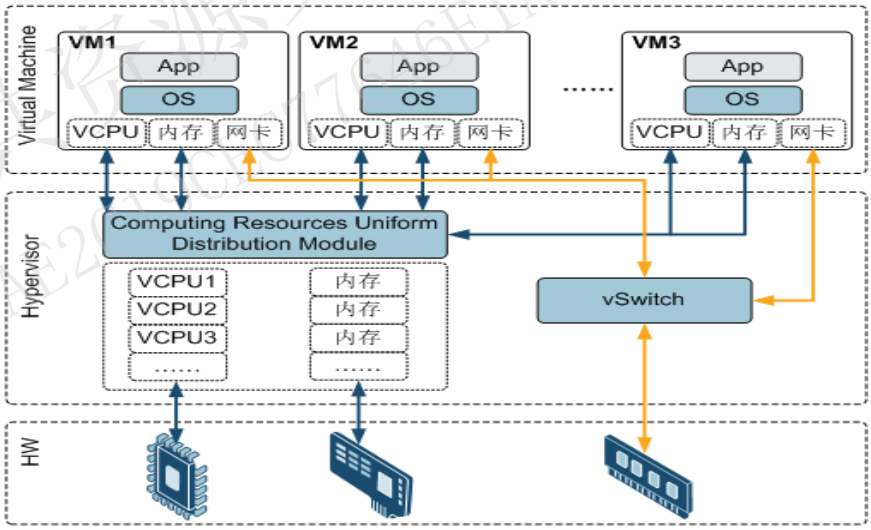
备实时对流量进行识别和净化，将 DDoS 攻击流量从混合流量中分离、过滤。Anti-DDoS 系统能有效检测与防御流量型 DDOS 攻击（如 UDP Flood、TCP SYN Flood 等）、Web 型 DDOS 攻击（如 HTTP get /post flood 攻击，慢速攻击，TCP 连接耗尽攻击，TCP 空连接攻击等）、DNS 服务攻击、攻击/僵尸工具发起的分布式拒绝服务攻击。

3.2.4.2.5 安全计算环境

云用户在利用虚拟化技术带来好处的同时，也带来新的安全风险。首先是虚拟层能否真正地把虚拟机和主机、虚拟机和虚拟机之间安全地隔离开来，这一点正是保障虚拟机安全性的根本。根据云计算领域面临的威胁与挑战，本项目云平台提供涵盖虚拟机隔离、网络隔离安全等多个方面的安全方案。

（一）虚拟机隔离

Hypervisor 能实现同一物理机上不同虚拟机之间的资源隔离，避免虚拟机之间的数据窃取或恶意攻击，保证虚拟机的资源使用不受周边虚拟机的影响。终端用户使用虚拟机时，仅能访问属于自己的虚拟机的资源（如硬件、软件和数据），不能访问其他虚拟机的资源，保证虚拟机隔离安全。虚拟机隔离如下图所示：



虚拟机隔离

1. 物理资源与虚拟资源的隔离：Hypervisor 统一管理物理资源，保证每个虚拟机都能获得相对独立的物理资源；并能屏蔽虚拟资源故障，某个虚拟机崩溃后不影响 Hypervisor 及其他虚拟机。

2.vCPU 调度安全：CPU 架构为了保护指令的运行，提供了指令的 4 个不同 Privilege 特权级别，术语称为 Ring，优先级从高到低依次为 Ring 0（用于运行操作系统内核）、Ring 1（用于操作系统服务）、Ring 2（用于操作系统服务）、Ring 3（用于应用程序），各个级别对可以运行的指令进行限制。vCPU 的上下文切换，由 Hypervisor 负责调度。Hypervisor 使虚拟机操作系统运行在 Ring 1 上，有效地防止了虚拟机 Guest OS 直接执行所有特权指令；应用程序运行在 Ring 3 上，保证了操作系统与应用程序之间的隔离。

3.内存隔离：虚拟机通过内存虚拟化来实现不同虚拟机之间的内存隔离。内存虚拟化技术在客户机已有地址映射（虚拟地址和机器地址）的基础上，引入一层新的地址——“物理地址”。在虚拟化场景下，客户机 OS 将“虚拟地址”映射为“物理地址”；Hypervisor 负责将客户机的“物理地址”映射成“机器地址”，再交由物理处理器来执行。

4.内部网络隔离：Hypervisor 提供 VRF（VPN Routing and Forwarding）功能，每个客户虚拟机都有一个或者多个在逻辑上附属于 VRF 的网络接口 VIF（Virtual Interface）。从一个虚拟机上发出的数据包，先到达 Domain 0，由 Domain 0 来实现数据过滤和完整性检查，并插入和删除规则；经过认证后携带许可证，由 Domain 0 转发给目的虚拟机；目的虚拟机检查许可证，以决定是否接收数据包。

5.磁盘 I/O 隔离：虚拟机所有的 I/O 操作都会由 Hypervisor 截获处理，Hypervisor 保证虚拟机只能访问分配给该虚拟机的物理磁盘，实现不同虚拟机硬盘的隔离。

（二）网络安全隔离

云平台采用 FusionSphere 解决方案。本次项目建设通过配合使用 FS 中的 VPC、安全组、DHCP 隔离等多个机制，共同保障云平台中虚拟化网络隔离的安全。

1.VPC：FusionSphere OpenStack 解决方案提供 VPC（Virtual Private Cloud）功能。一个 VPC 相当于一个局域网，用户通过配置不同 VPC，实现虚拟机之间的通信隔离，以增强虚拟机的安全。

2.安全组：FusionSphere 解决方案提供安全组功能。通过配置安全组，终端用户可自行控制虚拟机互通和隔离关系，以增强虚拟机的安全性。用户可通过配

置安全组规则，实现虚拟机间的互通或隔离，虚拟机之间通信和隔离原则如下：

- 属于同一个安全组的虚拟机，默认全部互通。
- 属于不同安全组的虚拟机，默认全部隔离。
- 仅安全组允许的访问请求，才能访问该安全组中的虚拟机。
- 用户可配置的安全组规则如下：
- 组间授权：允许哪些安全组访问本安全组。
- 虚拟机授权：允许哪些对端网络设备访问本虚拟机。

3.DHCP 隔离：FusionSphere 支持对虚拟机的 DHCP 隔离。如果用户在某台虚拟机中安装 DHCP 软件，开启端口组的 DHCP 隔离功能，可以防止该虚拟机通过安装的 DHCP 软件，为其他虚拟机分配 IP 地址，影响其他虚拟机的正常运行。

4. DHCP Snooping：DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。截获和解析虚端口上收到的 DHCP ACK 消息，将 DHCP Server 分配的 IP 记录下来，保存到 IP 和 MAC 绑定表，该 IP 和 MAC 绑定表与虚端口关联。

5.网络平面隔离：云平台安全解决方案的网络通信平面划分为业务平面、存储平面和管理平面，且三个平面之间是隔离的。保证管理平台操作不影响业务运行，最终用户不破坏基础平台管理。

（三）主机安全防护

云平台环境中使用了大量 OS、DB、Web 等公共应用软件，主机很容易遭受病毒入侵、漏洞攻击、木马等安全威胁，从而影响系统运营。云平台主机安全主要通过系统加固、主机安全防护、安全补丁等措施来提供保障。

1.主机安全防护系统：本项目配置计算安全管理平台，实现云平台的云管理节点、管理终端节点进行病毒防护、漏洞管理、主机安全检测等。云平台业务节点采用华为自研 Euler OS，并进行加固，安全性已经比较高。

2.虚拟机漂移绑定：在虚拟化资源池中由于虚拟机资源的弹性可变，因此经常发生由于资源枯竭等原因导致的虚拟机从不同的安全域之间反复漂移的情况。本次选用的系统采用独有的轻代理部署方式，在虚拟机中植入轻型代理，轻代理安全策略和虚拟机无缝绑定，无论虚拟机漂移至虚拟化资源池中的任何宿主机均可保证虚拟机防护策略稳定有效，提供虚拟机对虚拟机之间的攻击防护能力。

3.入侵防御：提供虚拟机逃逸检测、文件完整性监控、登录爆破检测和勒索软件防护，能够实时、准确地感黑客入侵事件，并提供黑客入侵的响应手段，有效防止管理面入侵。

4.风险评估：通过对服务器/虚拟机系统进行安全评估，分析系统存在的各种风险（账户、端口、软件漏洞、弱口令等），提示用户及时加固，消除安全隐患。

5.等保合规：计算安全平台提供基线检查、漏洞管理和入侵检测功能，帮助企业构建服务器安全体系，满足等保合规要求。

（四）应用安全防护

本项目的云解决方案中计算节点、管理节点底层均使用 EulerOS 操作系统，FusionSphere、ManageOne 等应用均使用了 Web 中间件及华为自研 GaussDB 数据库，为保证应用的安全性为保证此类设备的安全。

1.云平台安全加固：对应用底层 EulerOS 操作系统进行基础的安全配置，基础安全配置的主要内容如下：

- 最小化服务：关闭不必要的服务，如屏蔽Telnet服务和FTP服务。
- 服务加固：如加固SSH的服务。
- 内核调整：如关闭内核转发功能
- 文件目录权限设置：控制关键文件和目录的访问权限。
- 系统认证和授权：限制系统访问权限
- 帐号口令安全：管理用户密码。
- 记录操作日志：开启系统日志功能等。
- Web中间件的加固内容主要包含：
- 删除无关资源：删除预安装中间件时提供的示例性应用等。
- 限制平台信息泄露：屏蔽向客户端显示的中间件版本等。
- 保护关键端口：关闭shutdown端口等。
- 保护关键配置文件：控制关键配置文件权限等。
- 记录日志：创建自己的日志profile文件等。
- connector安全配置：配置SSL协议等。
- GaussDB数据库的加固内容主要包括：
- 连接配置：配置最大连接数、修改默认端口等。

公共资源交易平台技标专用

- 用户角色及密码：评估未知角色、密码复杂度等。
- 鉴权设置：配置口令加密策略、SSL算法等。
- 日志配置：配置记录日志等。
- 开发人员选项：关闭开发人员选项等。

2.WAF:为防范愈发严重的 Web 攻击，在核心交换区的 border-leaf 上旁路部署两台 WAF 设备，通过策略路由的方式，将前往 Web 服务器的流量引流到 WAF，实现对于 WEB 应用层的防护。基于规则的保护能对于大量的已知攻击提供精确的、细致的防护。其中能防护包括 SQL 注入、跨站脚本、操作系统命令注入、远程文件包含攻击、本地文件包含攻击、目录遍历、HTTP 协议违规、WEBSHELL 等类型的攻击。

（五）数据安全防护

数据安全是安全的重点，确保租户的关键/敏感数据（静态和动态）受到保护，以降低数据泄露和受损的风险，从而影响其云上业务系统的可靠性和安全性。云平台保障不同租户之间的数据隔离及安全共享，从传输安全、数据存储安全、容灾备份等技术手段加强数据安全保护，并通过数据库审计系统对访问数据库服务器的行为进行全方位审计。

1.传输安全：数据在传输过程中可能遇到被中断、复制、篡改、伪造、窃听和监视等威胁，需要保证信息在网络传输过程的完整性、机密性和有效性。传输安全由以下几个方面保证：

- 系统管理员访问管理系统时，对含有敏感数据的页面采用HTTPS方式，传输通道采用TLS加密。
- 用户访问虚拟机，采用SSH、RDP等加密方式。
- 远程运维时，采用安全加密的SSL VPN/IPSec方式。

通过加密的协议进行登录访问，可以进行有效的加密传输和身份认证，确保数据发送到正确的客户机和服务器，防止数据中途被窃取且保证数据的完整性。

2.数据安全存储：华为云安全解决方案配合 Fusionsphere 特性，从数据隔离、访问控制、数据可靠性以及剩余信息保护多个角度保障虚拟化环境中的数据存储安全。华为 Pacific 分布式存储提供存储加密能力，保障云上应用和数据库等的高安全数据存储能力。

公共资源交易平台投标专用

3.隔离用户数据：通过虚拟化层实现虚拟机间存储访问隔离，隔离用户数据，防止恶意虚拟机用户盗取其他用户的数据，保证用户数据安全。华为 Hypervisor 采用分离设备驱动模型实现 I/O 的虚拟化，虚拟机所有的 I/O 操作都会由 Hypervisor 截获处理；Hypervisor 保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。该模型将设备驱动划分为以下三部分：

- 前端驱动程序：在DomainU中运行，负责将DomainU的I/O请求传递到Domain0中的后端驱动。
- 后端驱动程序：在Domain0中运行，解析I/O请求并映射到物理设备，提交给相应的设备驱动程序控制硬件完成I/O操作。
- 原生驱动：在Domain0中运行。

4.控制数据访问：系统对每个卷定义不同的访问策略，没有访问该卷权限的用户不能访问该卷，只有卷的真正使用者（或者有该卷访问权限的用户）才可以访问该卷，每个卷之间是互相隔离的。

- 存储采用数据增强技术，系统会将存储池空间划分成多个小粒度的数据块，基于数据块来构建RAID组，使得数据均匀地分布到存储池的所有硬盘上，然后以数据块为单元来进行资源管理。
- 删除VM或删除数据卷，系统会进行资源回收，小数据块链表将被释放，进入资源池。存储资源重新利用时，再重新组织小数据块。通过这种方式，重新分配的虚拟磁盘恢复原来数据的几率小，有效做到了剩余信息保护。
- 系统进行资源回收时，支持对逻辑卷的物理Bit位进行格式化，保证数据的安全。
- 数据中心的物理硬盘更换后，需要数据中心的系统管理员采用消磁或物理粉碎等措施保证数据彻底清除。

5. 镜像和快照安全

云平台利用单向哈希算法保障镜像及快照数据完整性。

6.存储数据可靠性

云平台的数据存储采用可靠性机制，每一份数据都可以有一个或者多份

公共资源交易平台投标专用

副本，即使存储载体（如硬盘）出现了故障，也不会引起数据丢失，则不会影响系统正常使用。

错误!未找到引用源。章节。

（六）数据库审计

安全审计系统包含了数据库审计模块，其主要的功能包括“静态审计、实时监控与风险控制、实时审计、双向审计、审计规则、行为检索、关联审计、审计报表、安全事件回放、审计对象管理、预警管理、系统配置管理”等几个部分。

通过数据流镜像的方式，对所有对于数据库访问的流量进行审计.

通过网络数据的采集、分析、识别，实时监控网络数据库的所有访问操作，同时支持自定义内容关键字、支持自定义协议监测、支持自定义端口监测，实现数据库操作的内容监测识别，发现各种违规数据库操作行为。

对于数据库的违法访问系统能及时通过各种形式进行报警，并能够还原非法访问的操作全过程，实现安全事件的准确全程跟踪定位，全面保障数据库系统安全。数据库审计系统也具有集中统一的整合分析能力和全面、系统的报告、分析能力，能够为用户提供全面的数据库访问安全分析报告。

（七）大数据安全

数据安全为数据湖提供数据生命周期内统一的数据使用保护能力。通过敏感数据识别、分级分类、隐私保护、资源权限控制、数据加密传输、加密存储、数据风险识别以及合规审计等措施，帮助用户建立安全预警机制，增强整体安全防护能力，让数据可用不可得和安全合规。

1.数据分类：系统支持分类管理，支持业务分类定义和管理，支持给数据资产标识分类。通过数据分类，来有效识别数据库内的敏感数据。提供数据分类的新建分类、新建分组。

2.数据脱敏：数据脱敏包含静态脱敏和动态脱敏，支持按工作空间、数据源类型、数据库、数据表等选择任务执行范围，匹配对应的执行规则策略；使用静态脱敏经常使用测试环境中；动态脱敏经常使用在接口环境中。

3.数据水印：通过对泄露数据文件解封，根据数据文件的完整度和水印信息痕迹来检测水印是否存在，快速识别水印标记信息（数据源地址、分发单位、负责人、分发时间等），从而对安全事件精准定位追责。

- 水印容量：支持嵌入大容量信息。
- 隐蔽性：嵌入水印后不会引起数据明显的降质，并且不易被察觉，不影响宿主数据的可用性。
- 鲁棒性：嵌入水印的数据可以抵抗一定的恶意攻击。
- 安全性：持有密钥者（嵌入水印用户）才可正确提取出水印。
- 动态更新能力：支持数据增量（行级）嵌入。
- 盲检测：水印溯源过程不需要任何原始数据和辅助信息，只有水印嵌入者才可正确提取出水印。

3.2.4.2.6 安全管理中心

云平台中不仅需要安全防护技术，更重要的是对网络的安全管理。若缺乏对整个网络安全状况的全面监控管理，网络中所配置的安全设备便成了信息孤岛，无法与网络安全管理者进行安全信息交互，从而无法充分发挥其安全功能。

1.系统管理：为了保障云平台系统正常运转，提高服务和维护水平，特别是要管理分布式的网络、系统环境，有必要使用一套全面的网络运维管理系统（华为 eSight 设备），制定相应的管理策略和制度，实现集中统一管理，并实现：

- 监测管理自动化，故障处理变被动为主动，主动发现系统问题，在最短的时间内实现故障报警，管理人员可以快速采取解决措施。
- 完善的性能分析报告，更能帮助系统管理人员及时预测、发现性能瓶颈，提高系统的整体性能。
- 帮助管理者制定并执行良好的实施、管理和分析策略，使系统运维管理水平上升到新的高度。
- 通过部署统一网管（华为eSight设备）对系统的资源和运行进行配置、控制和管理，包括：
- 用户身份管理：统一管理系统用户身份，按照业务上分工的不同，合理地把相关人员划分为不同的类别或者组，以及不同的角色对模块的访问权限。权限设置可按角色划分，角色分为普通用户、系统管理员、安全管理员、审计管理员等。
- 系统资源配置与监控：进行系统资源配置管理与监控，包括CPU负载、磁盘使用情况、服务器内存、数据库的空间、数据库日志空间、SWAP使

用情况等，通过配置采样时间，定时检测。

- 系统加载和启动：进行系统启动初始化管理，保障系统的正常加载和启动。
- 系统运行的异常监控：系统资源和设备受到攻击，或运行异常时，会以告警等信息方式，通知管理员。安全管理平台可提供多种自动处理机制，协助用户监控最新告警，全方位掌控网络异常和攻击。
- 数据备份与恢复：数据的定期备份与恢复管理，识别需要定期备份的重要业务信息、系统数据及软件系统，规定备份信息的备份方式、备份频度、存储介质、保存期等，根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，定期执行备份与恢复策略。
- 系统管理员身份认证与审计：对系统管理员进行严格的身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

2.日志审计管理：数据中心环境平台部署日志审计系统（ISAP），提供各种资源（包含网络设备，安全设备）操作记录及安全事件的收集、存储和查询功能，存储满足 180 天。

3. 态势感知与安全管理中心：数据中心云平台需要具备安全运营能力，同时针对攻击要有检测处置能力；部署安全监控分析平台（ISAP），收集云内数据，实时监控资源的安全态势，识别潜在的风险，让安全运营者清晰、直观的看见威胁、感知风险、控制影响，为云安全保驾护航。构建事件响应处置能力（SOC），云业务安全运营团队在日常运营、重大保障等场景中进行告警、事件管理、指令及情报协同的统一作战工作台，支持安全编排，自动响应处置安全事件。

4.堡垒机：在管理区部署运维堡垒机，实现对云平台内云平台、安全产品、网络设备、服务器、存储等资源的帐号、认证、授权和审计的集中控制和管理。系统提供运维权限管理，完善的日志审计功能，支持对图形终端、字符终端、数据库应用、文件传输等。提供实时视频监控录屏，对高危的操作（删除或重启等）可以实时的截断。通过部署堡垒机来实现运维日志审计功能。

5.漏洞扫描：云平台平台部署漏洞扫描系统，通过扫描等手段对指定的虚拟机或者物理机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测

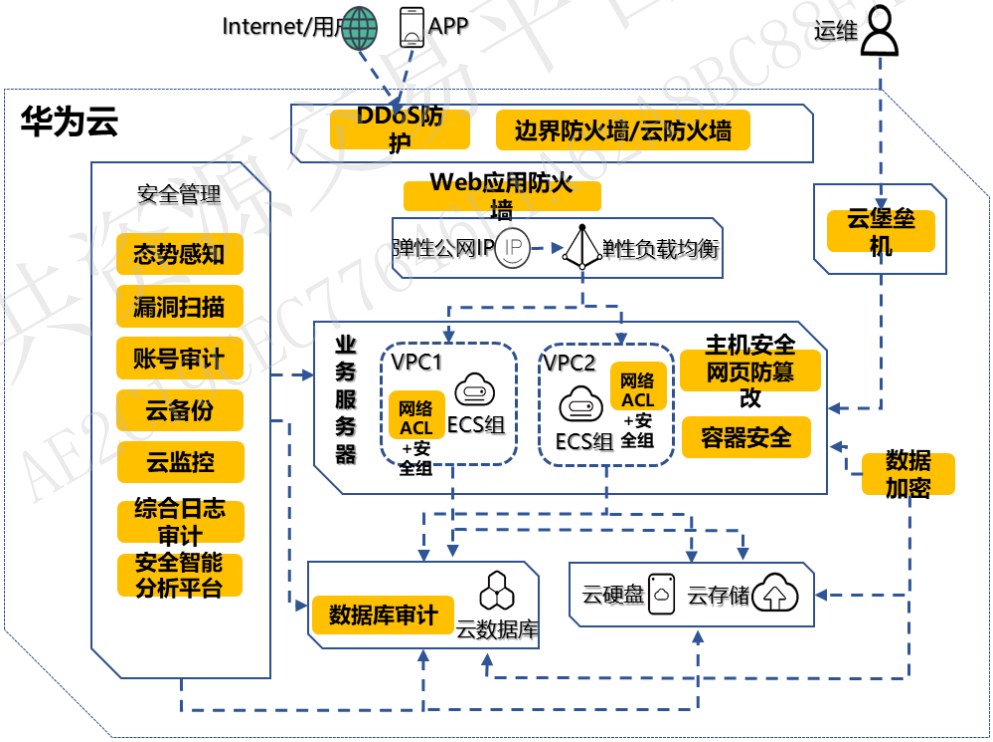
公共资源交易平台投标专用

（渗透攻击）行为，并提供及时的安全防护。漏洞扫描系统和防火墙、入侵检测系统互相配合，通过对网络的扫描，平台管理员能了解平台的安全设置和运行的应用服务，及时发现安全脆弱性，客观评估网络风险等级。平台管理员能根据扫描的结果更正网络安全脆弱性和系统中的错误设置，在黑客攻击前进行防范。漏洞扫描就是一种主动的防范措施，能有效避免黑客攻击行为，做到防患于未然。

3.2.4.3 租户安全建设方案

3.2.4.3.1 租户安全架构

对明确安全定级为三级的租户业务系统，可以选择用户集成安全套餐的安全服务基础防护包（云主机防护、云堡垒机、云 WAF、云数据库审计、漏洞扫描服务、秘钥管理服务、综合日志审计），以满足等保三级的预警、防护、检测、审计、响应需求。如下图所示：其中 DDOS，边界防火墙，态势感知、SOC 等复用平台安全能力。



租户安全架构

（一）安全通信网络

1. 在边界防火墙上开启 SSL VPN/IPSEC VPN，实现租户业务的安全接入。

2. 租户侧部署高性能负载均衡、专线、NAT 网关等满足租户业务的承载能力。

3.租出侧采用 VPC 实现网络的安全隔离，并通过 vFW 实现 VPC 之间的安全配置。

4.租户侧的应用，如 OBS，MYSQL 等访问，采用 HTTPS 加密访问，保障通信安全。

（二）安全区域边界

1.租户 VPC 之间互通，通过 ACL 进行安全访问控制

2.提供 VPC Endpoint 实现 VPC 服务的提供和访问控制

3.ELB 服务提供 VPC 业务访问，白名单控制能力

4.复用平台 AntiDDOS,提供 EIP 的流量清洗和检测

5.复用平台网络流程审计，实现 EIP 流量的安全审计

6.复用平台边界防火墙，部署 IPS 以及 AV 防病毒，实现 EIP 流量的入侵防御和防病毒

7.每个租户拥有独立的云堡垒机和日志审计，实现对自身业务的安全审计和边界访问控制。

（三）安全计算环境

1.部署统一认证系统 IAM，实现租户账户的统一管理和鉴权，角色管理、权限控制。

2.部署云堡垒机，实现租户业务运维的接入认证、行为审计。

3.部署数据库审计，采用旁路监听的方式，不影响业务的情况下对数据库进行审计。

4.部署日志审计系统，对租户日志进行采集、存储和分析。

5.部署主机安全服务，实现对主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能

6.部署云 WAF，防止数据泄露，抵御 CC 攻击，保护网站安全。

7.传输完整性，租户业务系统采用 HTTPS 或者 TLS 进行安全加密传输

8.存储完整性，块存储、对象存储、文件存储，大数据存储等进行校验，保证数据完整性。

公共资源交易平台投标专用

9.块存储实现存储池的加密能力，让 ECS 以及云数据库无感知加密。

10.部署 KMS 秘钥管理系统，为系统加密提供秘钥的安全性存储。

11.云备份，通过 LAN-FREE 备份，不用在云主机中安装 angent 即可实现备份，最大化减少对业务的影响。

（四）安全管理中心

1.部署租户云资源监控管理系统，实现租户云资源的性能、告警、容量等可视化监控，并能设置阈值告警能力。

3.2.4.3.2 虚拟防火墙

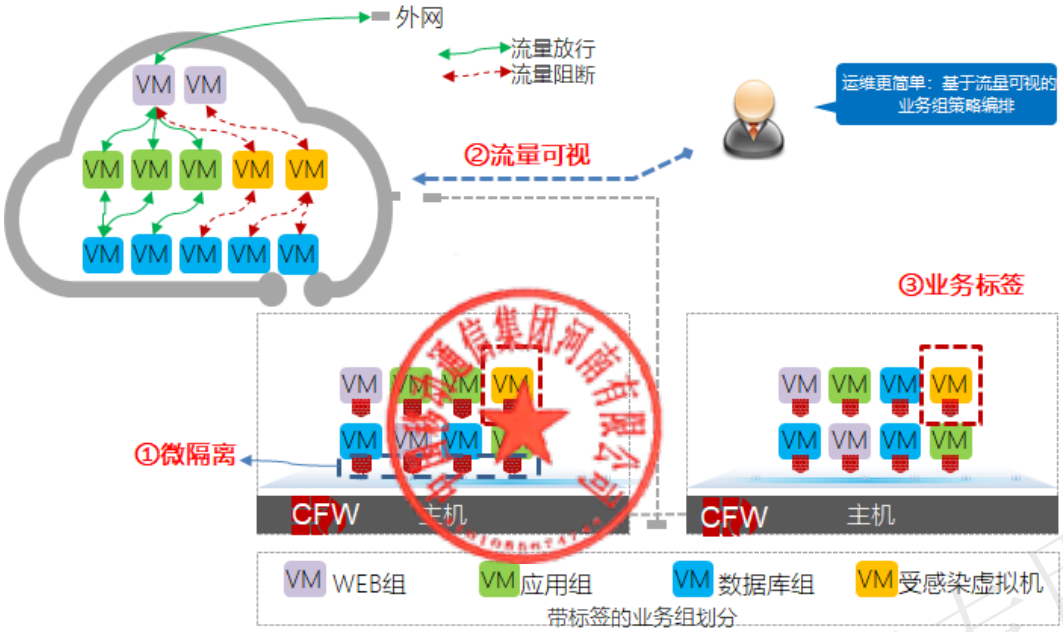
云防火墙（Cloud Firewall）为租户 VM 提供微隔离能力，并通过流量可视化、基于业务属性标签的安全策略配置手段来降低安全运维复杂度。云防火墙服务依赖分布式的 iptables 相关能力实现。

功能特点：

- 微隔离：提供 VM 到 VM 级细粒度的访问规则配置能力
- 流量可视：基于拓扑图访问关系辅助用户定义策略
- 业务标签：基于业务标签进行防护对象定义

安全管理员可以使用云防火墙，为业务提供基于 VM 粒度的安全防护，基于业务标签来定义安全策略，使用流量可视功能辅助策略配置，从而实现简化运维复杂度，提升防护效果。

公共资源交易平台投标专用
AE2C19CE7C46E1A62A8C8EA14DB9



3.2.4.3.3 虚拟漏洞扫描

漏洞扫描服务主要适用于以下场景：

（1）综合漏洞探测和弱口令检查：

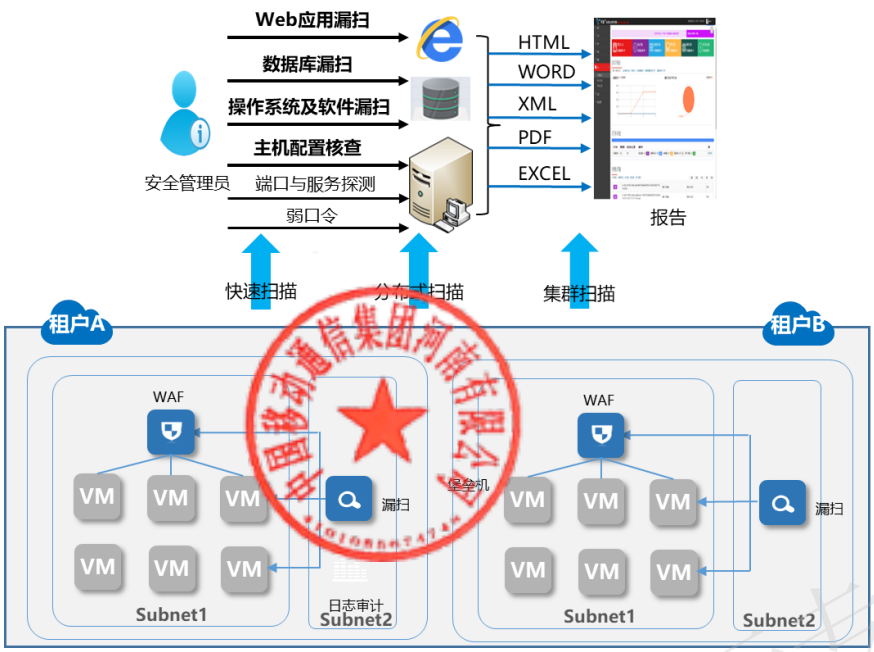
支撑 Web 应用弱点扫描、数据库弱点扫描、系统弱点扫描、应用软件安全检测，弱口令、端口与服务探测等综合漏洞探测。

支持对 FTP、TELNET、POP3、SMB、SSH、ORACLE、SMTP、IMAP、Mysql、MSSQL、DB2、、REDIS、RLOGIN、RDP、RTSP 等协议的弱口令检查。

（2）提供综合风险评估报告及漏洞修复建议

提供对租户资产的风险评估报告，对每个漏洞提供涉及受影响资产、漏洞等级、CVSS 评分、漏洞的详细描述，以及针对该漏洞的修复建议。租户用户可以基于报告的修复建议进行系统加固。

公共资源交易平台投标专用



云漏洞扫描流程图

漏洞扫描服务提供如下功能：

漏扫支持能力

Web、数据库、基线核查、操作系统及应用软件、弱口令、端口探测与服务识别 5 大扫描功能

分布式集群

分布式集群管理模块：漏洞扫描服务集成了 Web 扫描、系统扫描、基线核查、数据库扫描等，转化成 B/S 扫描框架，扫描更稳定、更快速、更易于扩展。除此之外，为了更大程度上实现快速扫描、分布式扫描，和以数百上千网站为目标的集群扫描，突破原本单机扫描器难以实现的批量扫描、集团网扫描障碍，在集成原引擎的前提下，实现了分布式集群管理模块，实现各引擎节点间任务的自由流转，高度智能分配资源，提高资源利用率

综合报表

统计报告内容同样支持用户自定义，极大程度上丰富了可用性与易用性。并且支持主流报告格式，包括：HTML、XML、PDF、WORD、EXCEL 五大报告格式。高度可视化的统计结果以及多维度的统计对比数据，标准的报告文档，让用户可以直观的看到自己的系统状态，报告文件告别人工修订

基线核查

安全配置核查系统帮助用户对云平台中租户资产的虚拟服务、物理服务

公共资源交易平台投标专用

器、网站中间件的配置文件进行自动化的检查，及时发现其中的安全威胁，并及时告知用户进行修正。

安全配置核查系统支持对 Windows 系列、Linux 系列、Unix 等操作系统进行安全基线检查；支持对 Tomcat，IIS，WebSphere，Apache，BIND 等中间件进行安全基线检查

3.2.4.3.4 虚拟堡垒机

云堡垒机（Cloud Bastion Host，CBH）是华为云 Stack 的一款 4A 统一安全管控平台，为企业提供集中的帐号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。云堡垒机提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。



云堡垒机流程图

账户管理：集中管理系统用户和资源帐号信息，对帐号全生命周期建立可视、可控、可管运维体系。

权限控制：集中管控用户访问系统和资源的权限，对系统和资源的访问权限进行细粒度设置，保障了系统管理安全和资源运维安全。

操作审计：基于用户身份系统唯一标识，从用户登录系统开始，全程记录用户在系统的操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。包括：

- Web浏览器运维
- 第三方客户端运维
- 自动化运维

高效运维：通过多种架构运维、多种运维资源、多种运维工具、多种运维形式的接入，全面提升运维效率。

3.2.4.3.5 虚拟主机安全

企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

企业主机安全服务（HSS）主要适用于以下场景：

- 等保必备：满足入侵检测、恶意代码防范、漏洞检测等条款
- 病毒防御：有效检测查杀勒索、挖矿、后门等恶意程序
- 主机加固：检测主机漏洞、弱密码等，根据结果进行加固
- 入侵检测：检测黑客入侵行为，应对高级威胁、红蓝对抗
- 安全运营：自定义安全策略积累固化安全团队实战经验；提供安全总览用于安全工作汇报，周边团队交流

公共资源交易平台技术专用



云主机安全防护流程

主机安全功能特性：

功能项	功能描述
资产管理	资产管理功能可深度扫描出主机中的账号、端口、进程、软件信息和自启动任务等。
漏洞管理	漏洞管理功能将检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞，帮助用户识别潜在风险。
入侵检测	入侵检测功能可识别并阻止入侵主机的行为，实时检测主机内部的风险异变，检测并查杀主机中的恶意程序，识别主机中的网站后门等。
基线检查	基线检查功能可扫描出主机系统和关键软件含有风险的配置信息。

表 0-8 主机安全特性

3.2.4.3.6 虚拟 Web 应用防火墙

Web 应用防火墙（云 WAF）服务主要应用于以下场景：

（1）防止数据泄漏

防止恶意访问者通过注入式攻击、网页木马、WebShell 等攻击手段入侵网

公共资源交易平台投标专用

站，窃取重要商业机密或敏感信息等，保护网站远离信息泄露风险；

（2）抵御 CC 攻击

当网站遭受 CC 攻击时，大量恶意请求长时间占用网站计算资源，导致网站业务响应缓慢甚至无法提供正常的服务，Web 应用防火墙可以精准识别 CC 攻击并过滤恶意请求，使普通用户能正常访问网站提供的业务；

（3）保护网站访客安全

Web 应用防火墙能识别跨站脚本（XSS）、网页木马、跨站请求伪造（CSRF）等攻击行为，除了保护自身安全以外，还能保护网站访问者的安全，避免信息泄露引起的纠纷和负面影响。

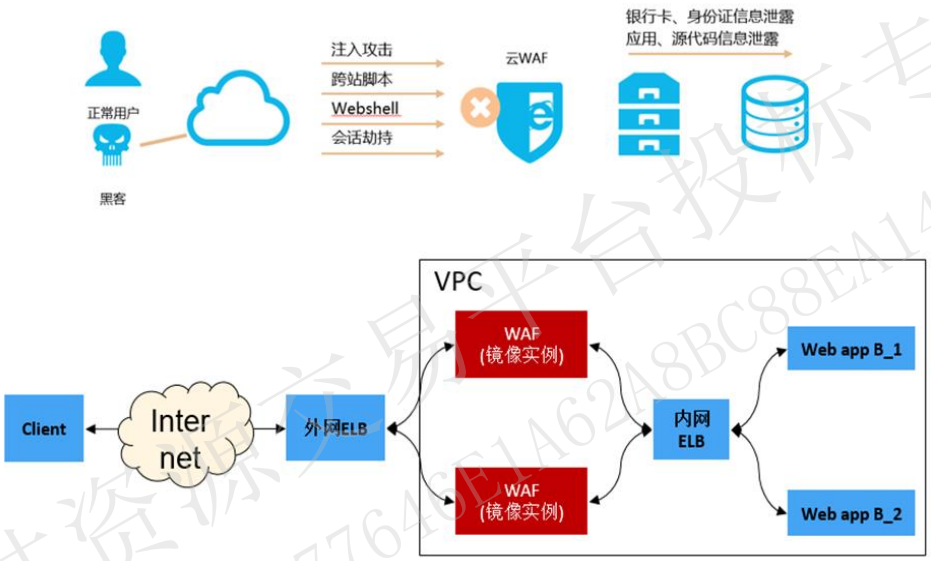


图 0-4 云WAF防护流程

功能特性如下：

功能项	功能描述
引擎实例管理	提供引擎实例订购与删除能力
防护网站管理	提供防护网站的创建、查询、修改和删除能力
防护策略管理	提供防护策略的创建、查询、修改和删除能力
事件查看	提供安全总览、详细事件日志查看、事件告警通知能力
Web防护	提供Web流量转发与攻击拦截的防护功能
运维告警	提供组件状态检查，资源告警的能力

表 0-9 WAF功能特性

3.2.4.3.7 网页防篡改

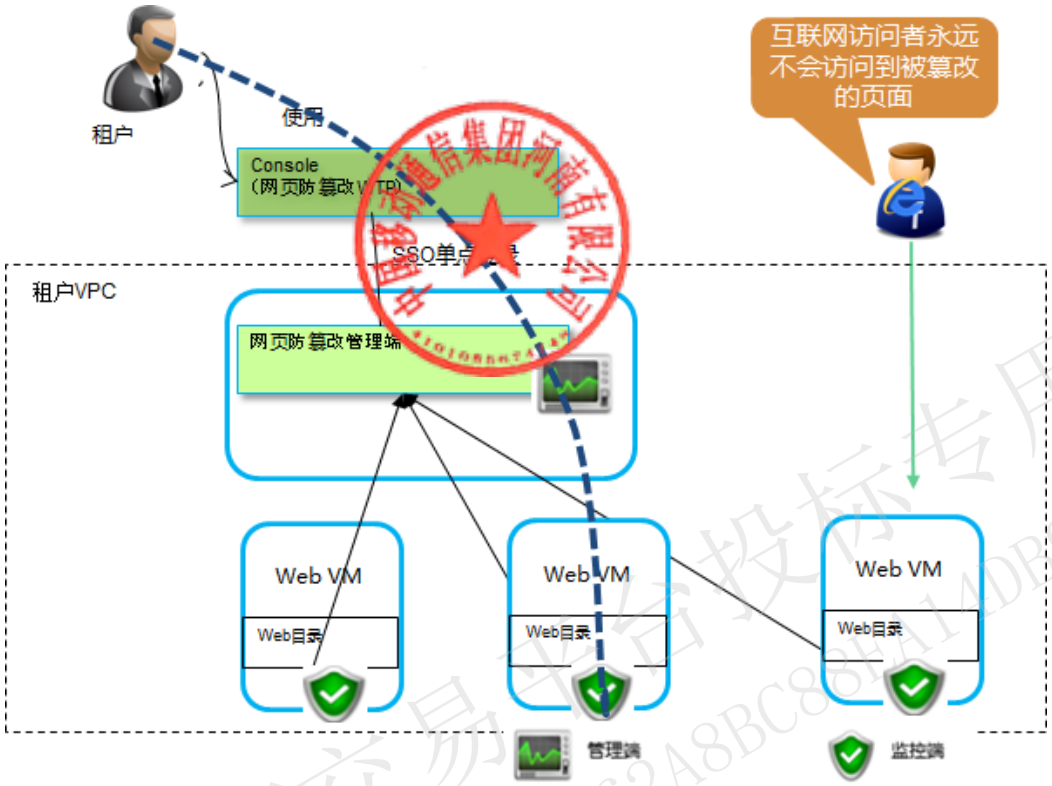
网页防篡改服务从系统底层驱动实现多种保护模式，防止静态和动态网站内容被非法篡改，保证网站内容的正确性。

网页防篡改服务提供如下功能：

- 网页文件保护：通过 web 防攻击模块、防篡改模块（系统内核层的文件驱动），可对动态和静态网页文件进行完美的保护。按照用户配置的进程及路径访问规则，设置网站目录、文件的读写权限，限制文件目录的增、删、改操作行为，确保网页文件不被非法篡改。
- 集中管理：通过监控端集中管理多台 Web 服务器，监测多主机实时状态，制定保护规则，接收 Web 服务器的报警和日志信息。控制 Web 服务器的启用、关闭、禁用等状态，并可对 Web 服务器的日志和报警情况做统计分析。
- 实时报警：对非法篡改行为，系统会自动记录报警日志，并通过手机短信、电子邮件、syslog 等多种方式通知管理员。能对网站攻击做到快速响应，及时应变。
- 管理员权限分级：可对管理员及监控端分配不同的权限组合。
- 日志审计：提供管理员行为日志，包括：时间、事件、操作对象、行为、IP 地址等详尽信息，方便区分正常更新过程还是篡改攻击行为；支持保护日志查询审计功能；用户不能进行日志修改、删除操作，确保日志的准确性与完整性。
- 站点文件保持：防篡改模块集成在 Web 服务器软件中，通过设定各种站点文件访问过滤规则，对多个站点文件或单个站点的文件夹进行保护。
- 系统信息检测：管理控制端机器能记录所有监控端 Web 服务器的 CPU、内存、硬盘等应用情况，方便管理员根据提供的硬件信息做升级和维护调整。

公共资源交易平台投标专用

- 系统自我保护：网页防篡改系统能够实时地保护自己，不被非法的删除、修改、卸载等，保证了即使服务器被非法入侵，也不能够对网站进行篡改，不能够对网站管理系统进行破坏。

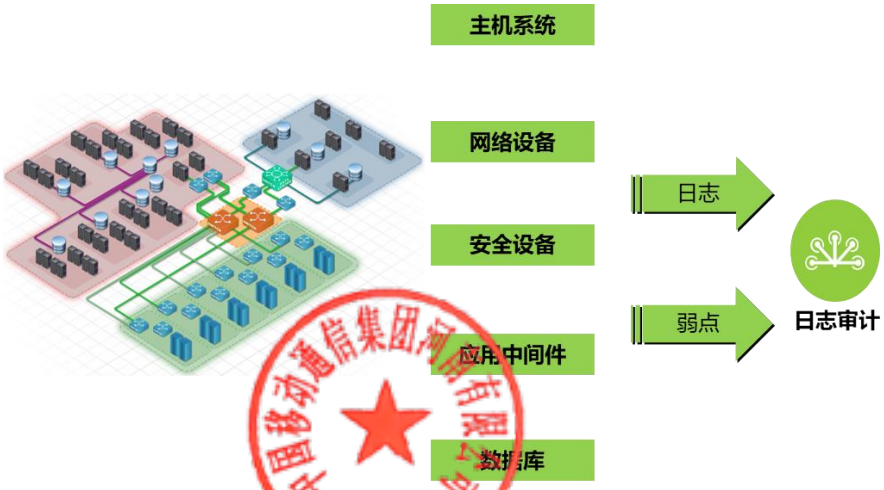


租户申请网页防篡改服务后，会在租户的业务网络拉起承载防篡改管理端的虚拟机，即防篡改安全实例。在防篡改管理端下载相应的防护客户端，部署在需要防护的 Web 服务器上，配置需要防护的 WEB 目录。在正常使用时，可以通过登录网页防篡改服务，通过单点登录的模式掉转到网页防篡改的客户端，配置使用。

3.2.4.3.8 虚拟日志审计

日志审计服务是信息系统的综合管理平台，通过对租户 ECS 主机、业务应用以及第三方在镜像市场上线的各种业务系统的日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保客户业务的不间断运营。

公共资源交易平台投标专用



云日志审计流程图

日志审计的主要功能如下：

全面日志采集

实现云上信息资产的日志获取，并通过预置的解析规则实现日志的解析、过滤及聚合。

智能关联分析

实现全维度、跨设备、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，客户可轻松实现各资产间的关联分析。

脆弱性管理

能够收集和管理来自各种 Web 漏洞扫描、主机漏洞扫描工具、网络漏洞扫描工具的产生的扫描结果，并实时和用户资产收到的攻击危险进行风险三维关联分析。

数据挖掘和数据预测

支持对历史日志数据进行数据挖掘分析，发现日志和事件间的潜在关联关系，并对挖掘结果进行可视化展示。系统自带多种数据统计预测算法，可以根据历史数据的规律对未来的数据发生情况进行有效预测。

可视化展示

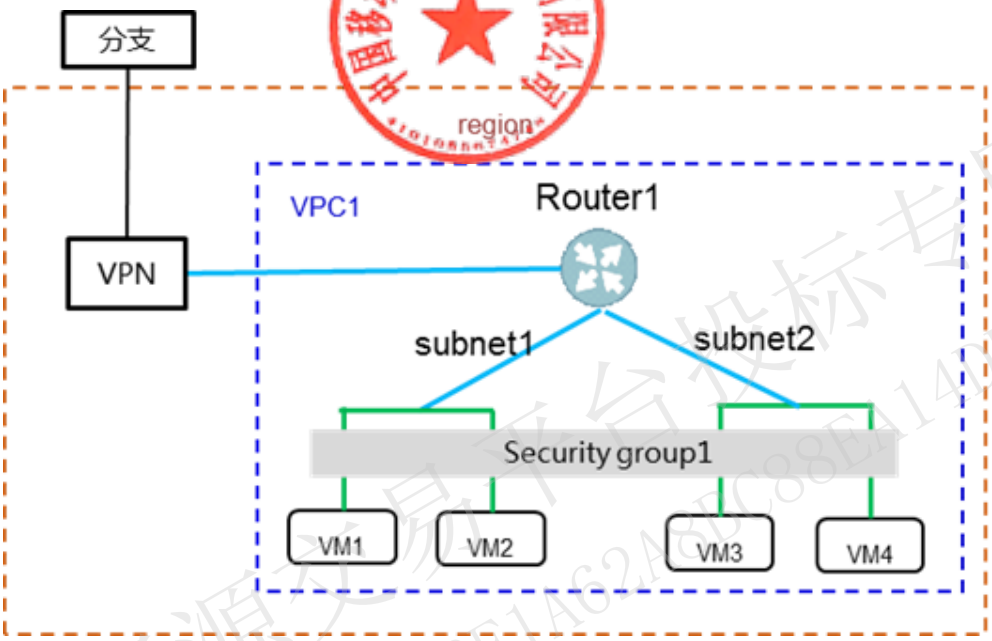
实现所监控的信息资产的实时监控、信息资产与客户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。通过各种事件的归一化处理，实现高性能的海量事件存储和检索优化

公共资源交易平台投标专用

功能，提供高速的事件检索能力、事后的合规性统计分析处理，可对数据进行二次挖掘分析。

3.2.4.3.9 虚拟 VPN 安全接入

虚拟 VPN 用于租户业务安全接入能力，VPN（Virtual Private Network）即虚拟专用网络，用于分支机构和 VPC 之间建立一条安全加密的通信隧道，把企业已有数据中心和云上的网络打通。



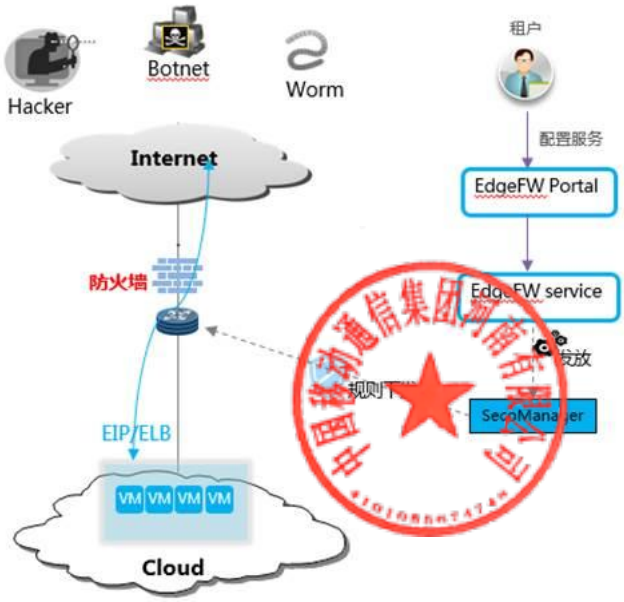
VPN业务流程

本项目提供 IPSec VPN 以及 SSL VPN 能力。

3.2.4.3.10 虚拟防病毒

边界防火墙服务主要适用于以下场景：

云数据中心与外部网络之间的南北向流量，为用户提供边界安全防护功能，帮助用户进行实时的云上边界安全高级防护，支持入侵防御和防病毒。



边界防火墙服务（Edge Firewall Service）针对云数据中心与外部网络之间的南北向流量，为用户提供边界安全防护功能，支持以弹性公网IP为防护对象的入侵检测防御（IPS）和网络防病毒（AV）功能。

边界防火墙服务的主要功能如下：

- 安全防护：可针对弹性公网 IP（EIP/ELB）进行南北向流量的访问控制、入侵防御和防病毒；
- 安全日志：根据源、目的地址、日期、攻击类型、协议等查看日志明细；
- 统计报表：图表的形式展示攻击类型、趋势、协议等排行。

3.2.4.3.11 入侵检测

网络检测与响应（Network Detection and Response，简称 NDR）是基于华为多年攻防经验，运用特征规则、大数据分析等技术，对企业网络流量进行实时检测、捕获、解码、审计，发现企业网络和系统中存在的安全风险和威胁，实现四到七层网络流量防护的安全平台。

公共资源交易平台投标专用

当主机遇到常见 Web 攻击时，NDR 通过分析 7 层协议（包括 HTTP/Redis/MySQL 等交互协议），对流经核心路由器的流量进行全量检测。当检测到一些恶意特征的流量时，NDR 通过构造阻断包，经核心路由器转发给攻击者和主机，从而阻断访问，为平台的主机提供安全防护，其主要架构如下图所示。



NDR 的阻断原理如下：

1. 攻击者的流量流入核心路由器，再由核心路由器转发给主机。
2. 同时，核心路由器的流量经分光器拷贝到 NDR。
3. NDR 通过检测确认为网络攻击后，发送构造的阻断包给核心路由器。
4. 核心路由器将构造的阻断包分别转发给攻击者和主机从而阻断攻击访问。

NDR 主要有以下功能：

- 攻击统计

  通过内置安全规则，精准识别爆破、SQL 注入、Log4j 等多种类型攻击访问，支持统计最近一小时内的攻击次数和攻击类型。

- 流量分析

公共资源交易平台投标专用
AE2019CE27646E1A62A8BC88EA14DB9

通过拷贝流经核心路由器的全部流量，实时分析并通过图表呈现不同时段流入和流出的流量值及所属 IP 等信息。

- 日志分析

  支持攻击事件日志、阻断日志、流量日志和审计日志，全面记录攻击源和攻击目的的详细信息，帮助运维人员精准定位网络攻击。

- 访问防护

  内置华为云平台多年攻防实战积累的经验规则，覆盖常见网络攻击，并持续运营刷新，有效保护资产，并提供观察和拦截两种防护模式。

- 威胁情报

  通过利用行业威胁情报和华为云自研的大数据量、高准确度的威胁情报库，锁定攻击 IP 的地理位置信息，为精准防护提供进一步的保障。

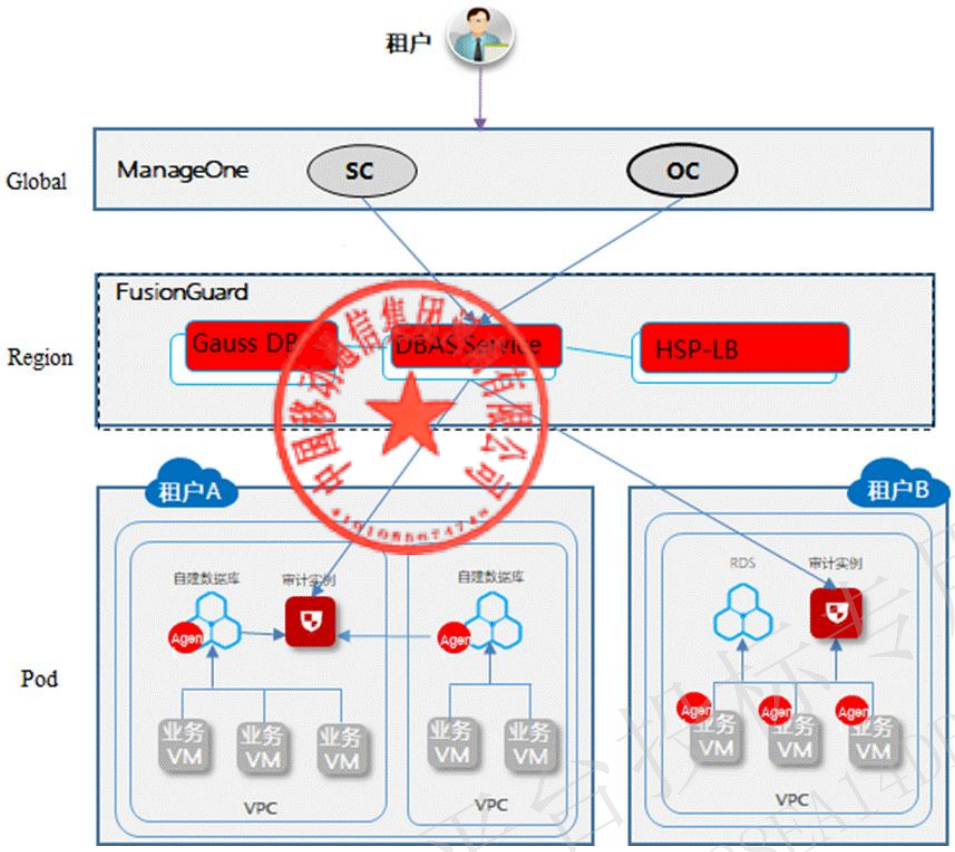
- 告警通知

  当前支持攻击告警通知，当网络攻击达到告警阈值，NDR 将以告警形式上报到 ManageOne 运维面，便于统一运维。

3.2.4.3.12 虚拟数据库审计

数据库审计服务(Database Audit Service)，为用户的基于 ECS/BMS 自建数据库、RDS 数据库，提供用户行为发现审计、多维度分析、实时告警和报表等功能，保障云上数据库的安全，满足用户合规要求。

公共资源交易平台投标专用
ADC13CE077646E1A62A8BC88EA14DB9



数据库审计流程

审计信息展示：数据库审计的审计内容包括会话的终端信息、会话的主机信息、会话的其它信息、操作信息等；支持从会话维度、语句类型纬度、风险纬度三个纬度进行导航展示，支持基于时间、客户端 IP、目标数据库 IP、客户端 MAC、目标数据库 MAC，操作类型、客户端端口、操作信息大小、返回状态、结果信息、客户端执行命令等详细信息内容。

审计报表：支持（系统级）多数据库聚合报表展现和单数据库综合性报表展现；支持基于总体概况、性能、会话、语句、风险多层面展现报表；支持报表定时推动功能，自定义推送周期推送报表文档；支持多种关联分析，对异常行为体统精细化报表，如会话（客户端和数据库用户）行为报表、风险操作风险分布情况分析报表、合规报表（满足数据安全标准如 Sarbanes-Oxley）等；

风险操作、攻击检测及告警：风险操作（操作类型、操作对象、风险等级等）告警；能够检测 SQL 注入（命令特征或风险等级）发现并告警；系统资源（CPU、内存和磁盘）阈值告警；支持自定义风险规则。

管理员三权分立：支持系统、安全、审计管理员三员权限分离，并基于云 IAM

进行统一身份认证管理；

隐私数据保护：用户可以通过内置规则或自定义规则对审计平台（审计日志）存储和展示的敏感信息脱敏；严控个人数据收集、存储；

合规及认证：国内：满足网安法、等保三级数据库审计需求，获得公安部《计算机信息系统安全专用产品销售许可证》；国外：满足 SOX、Sarbanes 等国外法案，通过 CSA STAR、ISO 27001、ISO27017、ISO27018 安全认证。

3.2.4.3.13 虚拟密码机

CHSM 云服务器密码机 （cloud-hosted hardware security module，简称 CloudHSM 或 CHSM） ，即在云计算环境下，采用虚拟化技术，以网络形式，为多个租户的应用系统提供密码服务的密码设备。

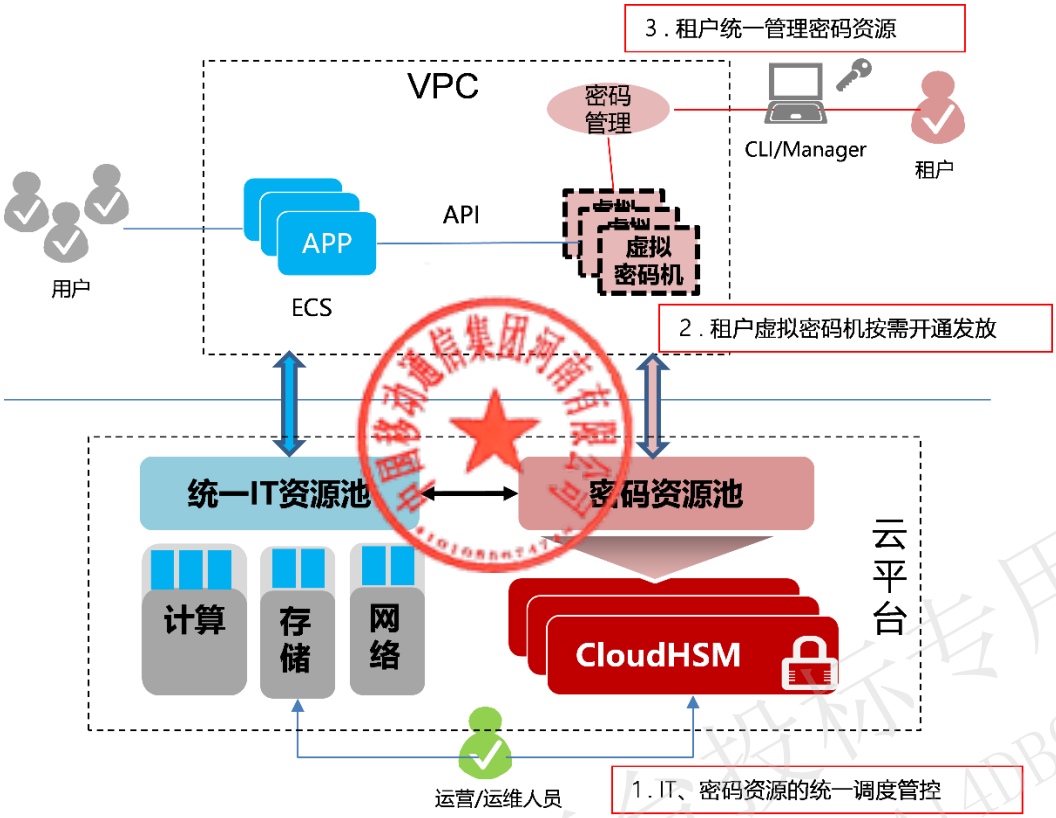
能够为政务云提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，可以满足通用密码服务，保证传输信息的机密性、完整性和有效性，司时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。

当前华为云 Stack 数据加密服务支持的云服务器密码机型号为兴唐通信 SJJ1811、卫士通 SJJ1744，设备均支持国密算法（SM2、SM3、SM4 等），并获得国家密码局认证。

3.2.4.3.14 数据库加密服务

数据加密服务（Data Encryption Workspace，简称 DEW）,基于国家密码局认证的云服务器密码机（CloudHSM），构建虚拟化密码资源池，实现 IT、密码资源统一调度管控，为用户按需提供虚拟密码机（VSM）的服务，支持政务、金融、公安等行业客户的云上密码服务及国密改造需求。解决了加密机入云、密码及 IT 资源统一调度、自动化管维的问题。

公共资源交易平台技标专用



数据加密服务基于云加密机在云平台侧实现了虚拟化密码资源池的构建，并可统一调度管理密码资源，实现 IT、密码资源的统一调度分配，支持对虚拟密码资源的配置、操作、漂移、升级等。租户在数据加密服务界面，可按需申请相应的 VSM 资源，服务自动化将 VSM 设备映射入租户 VPC，同时管理员将所需的管理、备份 Ukey 发放给用户。用户持 Ukey 登录管理配置工具，远程初始化、配置 VSM，并完成应用改造接入，实现应用对加密服务调用。租户可在服务界面进行 VSM 的申请、维护、关闭等，也可登录管理配置工具对名下所有密码设备、密钥进行统一管理和配置。

DEW 服务具有以下功能：

- 密码资源池的统一调度：
  - 实现密码资源池管控系统，基于 CloudHSM 构建密码资源池；
  - 支持对 CloudHSM、VSM 自动化配置、操作、漂移、升级等；
  - 支持对密码资源池统一监管、分配、运维、告警处置等；
  - 支持 VSM 集群集容量：>10240。
- 租户按需动态开通 VSM：

- 支持租户自动化开通、配置、关闭 VSM 资源；
- 支持租户 VSM 资源总览、性能查看、VSM 资源查看等；
- 单 VSM 加密性能规格：并发连接数 64、256 位 SM2 签名速度 ≥ 3200 次/秒、 SM4 加密/解密速度 ≥ 4000 次/秒、 SM3 杂凑计算性能≥ 4500 次/秒

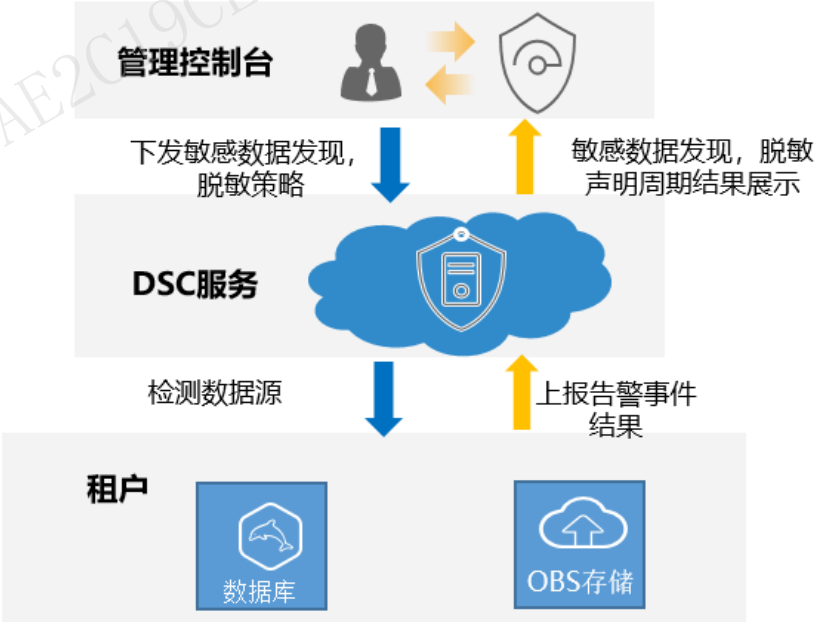
- 将 VSM 的安全接入租户 VPC：通过网络映射，将 VSM 接入租户 VPC，实现加密机的本地调用，保障 VSM 的使用、管理安全。
- 租户密码资源统一管理：支持租户统一管理名下的所有密码设备、密钥资源。

3.2.4.3.15 云资源监控

ManageOne 支持对云平台的各类云资源进行监控，提取各类云资源的监控指标，并支持设定阈值产生相应的阈值告警。

3.2.4.3.16 数据安全服务 DSC

数据安全中心服务（Data Security Center，DSC）是新一代的云化数据安全平台，提供数据分级分类、敏感数据识别、数据水印溯源和数据静态脱敏等基础数据安全能力，通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。



公共资源云易平台投标专用
AE2019CEC7164E1AC2A8BC88EA14DB5

敏感数据自动识别分类

从海量数据中自动发现并分析敏感数据使用情况，基于数据识别引擎，对其储存结构化数据（RDS）和非结构化数据（OBS）进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。

数据脱敏保护

通过多种预置脱敏算法+用户自定义脱敏算法，搭建数据保护引擎，实现非结构化数据脱敏储存，结构化数据静态脱敏，防止敏感数据泄露。

满足信息合规要求

DSC 拥有数十种合规模板，包含 GDPR，PCI DSS，HIPAA 等，多种合规规则一键匹配识别，生成报表供针对性整改，精准区分和保护个人数据，避免产生合规问题。

功能特性	说明
数据安全总览	展示数据安全全生命周期各个阶段的状态，包括云服务全景图、数据采集安全、数据传输/存储安全、数据使用安全和数据交换/删除安全，实时呈现了用户资产的具体情况。
资产列表	DSC 支持管理 OBS、数据库和大数据三类数据资产。
敏感数据识别	• **数据自动分级分类：**在 AI 和专家知识库的双重加权下，精准识别敏感数据和文件，覆盖结构化（RDS）和非结构化（OBS）两种数据类型，实现云上多场景覆盖。 – 文件类型：支持近 200 种非结构化文件。 – 数据类型：支持数十种个人隐私数据类型，包含中英文。 – 合规模板：多种内置合规知识库，如 GDPR，PCI DSS，HIPAA 等。

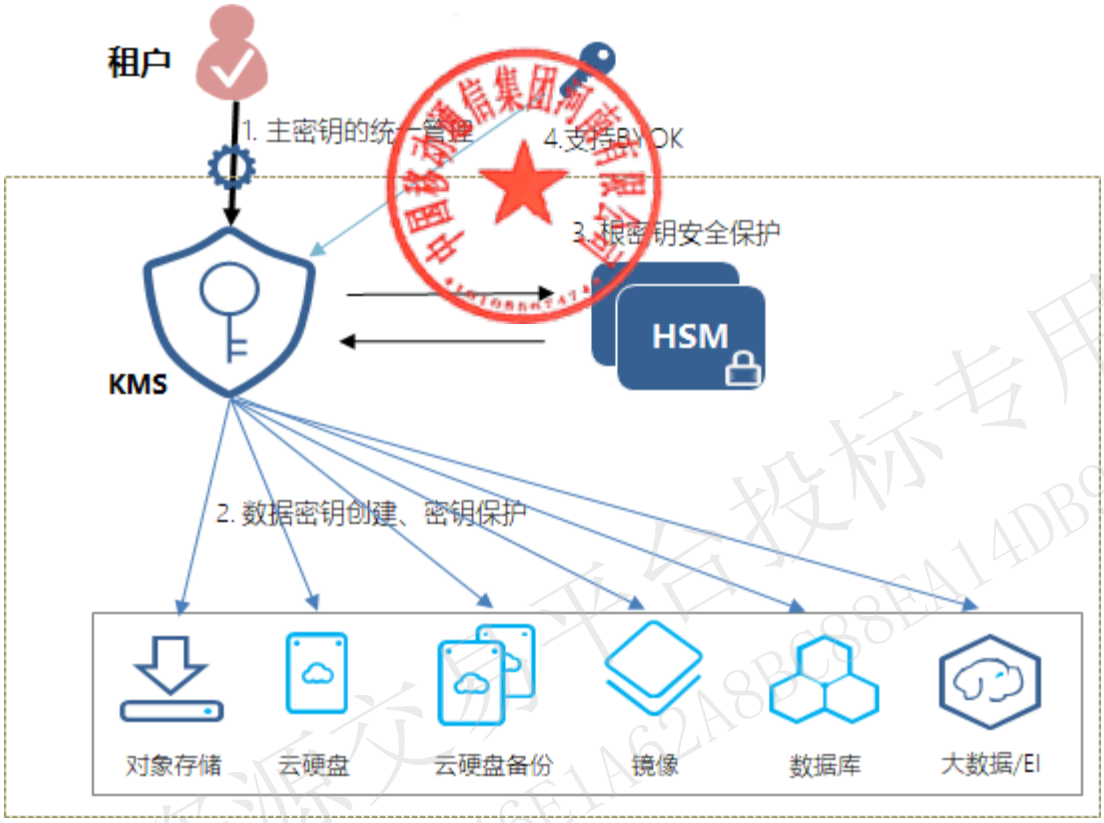
公共资源交易平台投标专用

功能特性	说明
	• **自动识别敏感数据** – 自动识别敏感数据及个人隐私数据。 – 支持自定义规则，场景适配不同行业。 – 血缘图梳理敏感文件框架，清晰定位。
数据脱敏	DSC 的数据脱敏支持静态脱敏和动态脱敏。 DSC 的数据静态脱敏特点： • 不影响用户数据：从原始数据库读取数据，通过精确的脱敏引擎，对用户的敏感数据实施静态脱敏，脱敏结果另行存放，不会影响原始的用户数据。 • 支持云上多种场景：支持 RDS，ECS 自建数据库，大数据。 • 满足多种脱敏需求：用户可以通过 20+种预置脱敏规则，或自定义脱敏规则来对指定数据库表进行脱敏实现一键合规。 同时，DSC 提供了数据动态脱敏的 API 接口供您使用。
数据水印	针对 PDF、PPT、Word、Excel 格式的文件提供了添加和提取水印的功能。 • **版权证明：**嵌入数据拥有者的信息，保证资产唯一归属，实现版权保护。 • **追踪溯源：**嵌入数据使用者的信息，在发生数据泄露事件时，追踪其泄露源头。

3.2.4.3.17 密钥管理服务 KMS

密钥管理服务（Key Management Service，简称 KMS）：为平台云服务、租户

业务应用提供一种安全可靠、简单易用的密钥托管服务，其密钥安全由硬件安全模块（HSM）保护，帮助用户集中管理密钥生命周期安全。解决了云服务加密密钥安全创建、租户密钥统一管理的问题，当前已支持 OBS、DWS、DAYU 服务集成加密功能。



用户可登录 KMS 系统，对租户住密钥进行全生命周期管理，包含创建、启用、禁用、删除、轮转、别名、修改用户主密钥等。对于集成了 KMS 加密的 OBS 服务，用户登录 OBS 服务时，可以选择“KMS 加密”加密文件，自动对上传文件加密保存在云端存储，下载时自动解密。

KMS 服务具有以下安全功能：

- 密钥生命周期管理：
  - 支持根密钥保护，基于硬件 HSM 根密钥保护。
  - 支持租户创建、启用、禁用、删除、轮转、别名、修改用户主密钥。
  - 支持各服务、应用创建、加密、解密数据密钥。
  - 支持 AES 256、国密 SM4 两类对称密钥的创建和管理。

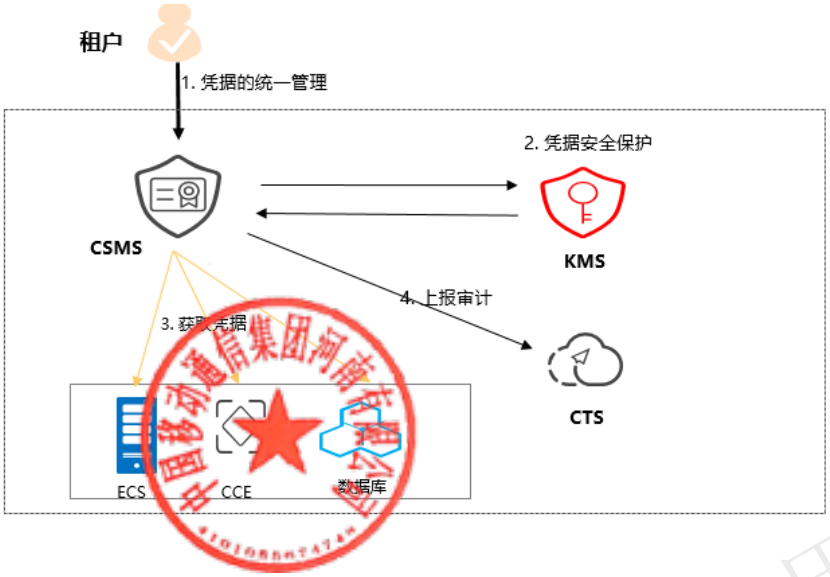
公共资源交易平台投标专用

- 云服务集成加密支持：
  - 对象存储服务（OBS）集成：一键开通文件加密功能，对上传/下载 OBS 文件进行服务端加密/解密，1 个文件 1 个密钥。
  - 智能数据湖运营平台（DAYU）集成：创建 MRS Hive、MRS Hbase、DWS、DLI、MySQL、SparkSQL、RDS 等数据连接时，自动调用 KMS 创建数据密钥加密数据连接口令等。
  - 数据仓库服务（DWS）集成：服务创建数据表时，自动调用 KMS 创建数据密钥加密数据表。
- 密钥安全管理：
  - 密钥轮转：用户可按需对主密钥进行轮转（支持轮转周期 7 天 ~ 1095 天）；
  - 密钥授权：支持按需密钥授权；
- 自主密钥导入（BYOK）：用户根据 KMS 提供的 API 接口导入用户自己生成或获取到的用户主密钥；
- 小数据加密：少量数据（如口令、证书等）需要加解密时，可利用 KMS 在线工具完成；

当前 KMS 已与国内主流的加密厂商 HSM 设备型号适配：支持江南天安 SJJ1310、三未信安 SJJ1212。

3.2.4.3.18 凭据管理服务 CSMS

公共资源交易平台技标专用
AE2C19CEC7646E1A62A8BC88EA14DB9



云凭据管理服务（Cloud Secret Management Service，CSMS），是一种安全、可靠、简单易用的凭据托管服务。用户或应用程序通过凭据管理服务，创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期和统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密以及权限失控带来的业务风险。

功能	服务内容
凭据全生命周期管理	• 创建、查看、定时删除、取消删除凭据 • 修改凭据的加密密钥和描述信息
凭据版本管理	• 创建、查看凭据版本 • 查看凭据值
凭据版本状态管理	更新、查询、删除凭据版本状态
凭据标签管理	添加、搜索、编辑、删除标签

以最基础的数据库用户名及密码管理为示例，为您介绍凭据管理服务基本的

使用场景。



流程说明如下：

步骤 1 您首先需要在凭据管理服务中使用控制台或者 API 创建一个凭据，用来存储数据库的相关信息（例如：数据库地址、端口、密码）。

步骤 2 当您使用应用程序访问数据库时，凭据管理服务会去查询步骤 1 所创建的凭据存储的内容。

步骤 3 凭据管理服务检索并解密凭据密文，将凭据中保存的信息通过凭据管理 API 安全地返回到应用程序中。

步骤 4 应用程序获取到解密后的凭据明文信息，使用这些安全的信息访问数据库。

----结束

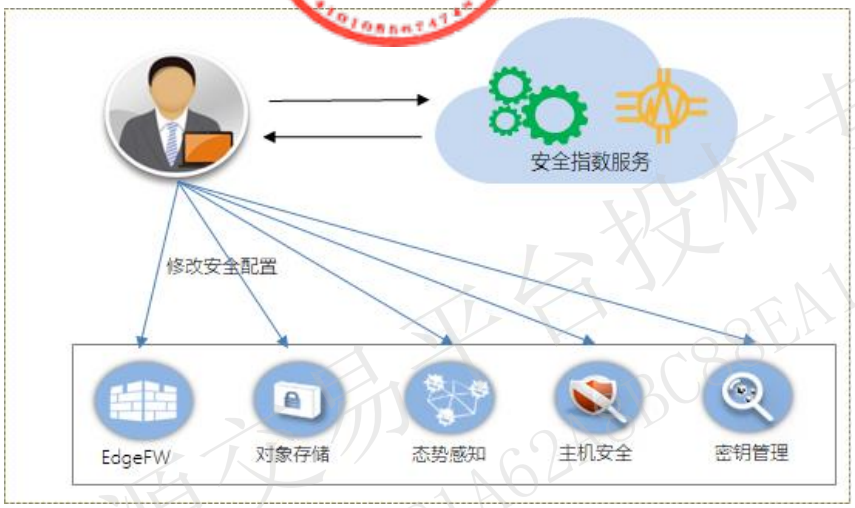
对其他云服务的依赖：凭据管理的安全能力强依赖于 KMS 服务，当前国内支持 KMS_江南天安、KMS_三未信安，国外 KMS_Utimaco。

3.2.4.3.19 安全指数服务 SIS

安全指数（Security Index Service，SIS）是关于云环境的一个安全评估服务，为用户提供统一、直观、多维度的安全视图。用户可以通过安全指数服务了解所使用云环境是否已合理配置，所采取的安全措施是否已经足够，以及主动安全、被动安全的概况。

公共资源交易平台投标专用

- 安全体检：从身份鉴别、访问控制、入侵防范、资源控制、备份恢复、数据安全几个维度对用户的云环境进行评估，根据最佳实践对不安全的配置提出修改建议，并提供快速修复的链接。
- 合规报告：根据等级保护规范的技术要求，从安全计算环境、安全通信网络维度对用户的云环境进行检测，提供合规检测报告，辅助用户做等保评估。
- 对云服务配置进行检查，依赖 OBS、VPC、BMS、ELB、HSS、VDC、ECS、CSBS、CSDR、KMS、DEW、EdgeFW、CFW 等服务。



3.2.4.3.20 安全云脑 SecMaster

安全云脑（态势感知）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。

公共资源交易平台投标专用



安全云脑功能介绍：

总览

总览呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。

功能模块	功能详情
安全评分	根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
安全趋势	呈现最近 7 天整体资产安全健康得分的趋势图。

工作空间管理

工作空间属于云脑顶层工作台，单个工作空间可绑定普通项目、企业项目和 Region，可支撑不同场景下的工作空间运营模式。

公共资源交易平台投标专用

功能模块	功能详情
工作空间	单个工作空间可绑定普通项目、企业项目和 Region，可支撑不同场景下的工作空间运营模式。

安全态势

支持通过安全态势即时查看大屏、定期订阅安全运营报告，了解安全运营核心关注指标。

功能模块		功能详情
态势总览	安全评分	根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
	安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
	安全趋势	呈现最近 7 天整体资产安全健康得分的趋势图。
安全大屏		利用 AI 技术将海量云安全数据的分析并分类，通过安全大屏将数据可视化展示，集中呈现云上实时动态，云上关键风险一目了然，掌握云上安全态势更简单，更直观，更高效。
安全报告		通过创建分析报告，及时掌握资产的安全状况数据。

公共资源交易平台投标专用

功能模块	功能详情
任务中心	集中呈现当前需要进行处理的任务。

资产管理

安全云脑支持对云上资产全面自动盘点，并呈现云上资产实时安全状态。

功能模块	功能详情
资产管理	同步所有资源的安全状态统计信息，支持查看资源的名称、所属服务、安全状况等，帮助您快速定位安全风险问题。

风险预防

风险预防提供基线检查和漏洞管理功能，帮助您的云安全配置达到等保等各类权威安全标准和华为云安全最佳实践标准；知晓全局的漏洞分布，并一键修复漏洞。

功能模块	功能详情
基线检查	1、通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。 2、当前仅支持云服务基线检查，比如 IAM、ECS、OBS、HSS、VPC、WAF、ELB、RDS、DCS、DDOS、VSS 和 CSS
漏洞管理	通过自动同步华为云主机安全服务（Host Security Service，HSS）漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议。

公共资源交易平台投标专用

威胁运营

威胁运营提供丰富的威胁检测模型，帮助您从海量的安全日志中，发现威胁、生成告警；同时，提供丰富的安全响应剧本，帮助您对告警进行自动研判、处置，并对安全防线和安全配置自动加固。

功能模块		功能详情
安全分析	查询与分析	• 检索分析：支持数据的快捷检索分析，支持安全调查场景安全数据的快速筛留、筛除等操作，快速定位关键数据。 • 筛选统计：支持数据字段快速分析统计，并基于分析结果进行数据的快速筛选；时序数据支持默认时间分区统计，快速识别数据量的变化趋势，支持基于时间分区的快速筛选；支持分析、统计、排序等丰富统计分析函数，支撑快速构建安全分析模型。 • 可视化：支持数据可视化分析，直观反映业务结构性和趋势性特征，并基于此构建自定义分析报告和分析指标。
	数据监控	支持数据流量端到端的监控管理。
数据监控		支持构建告警模型。
事件管理		集中呈现事件详情，支持人工转事件、自动化转事件。

公共资源交易平台供标专用

功能模块		功能详情
告警管理		提供统一的数据类管理（安全运营对象），内置华为云告警标准。通过集成各云服务告警，包含 HSS、WAF、DDoS 等，集中呈现告警信息。
情报管理		提供统一的数据类管理（安全运营对象），内置华为云威胁情报指标库标准。支持接入各云服务情报，同时也可以基于告警和事件自定义规则提取指标。

安全编排

安全编排支持剧本管理、流程管理、数据类管理（安全实体对象）和资产连接管理等。通过安全编排可以对安全响应剧本进行拖拽式的灵活编排，动态适配您的业务需求。也可以对安全运营的对象、交互的页面进行灵活扩展和定义。

功能模块	功能详情
运营对象	集中对数据类、数据类类型、分类映射等运营对象进行管理。
剧本编排	支持对剧本、流程、资产连接、实例的全生命周期管理。
页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。

数据集成

通过集成云原生安全产品，进行数据对接。集成后可以检索并分析所有收集

公共资源交易平台投标专用

到的日志。

功能模块	功能详情
数据集成	云内置采集系统，支持一键集成存储、管理与监管、安全等多种华为云云产品的日志数据。集成后，可以检索并分析所有收集到的日志。

3.2.4.3.21 安全组

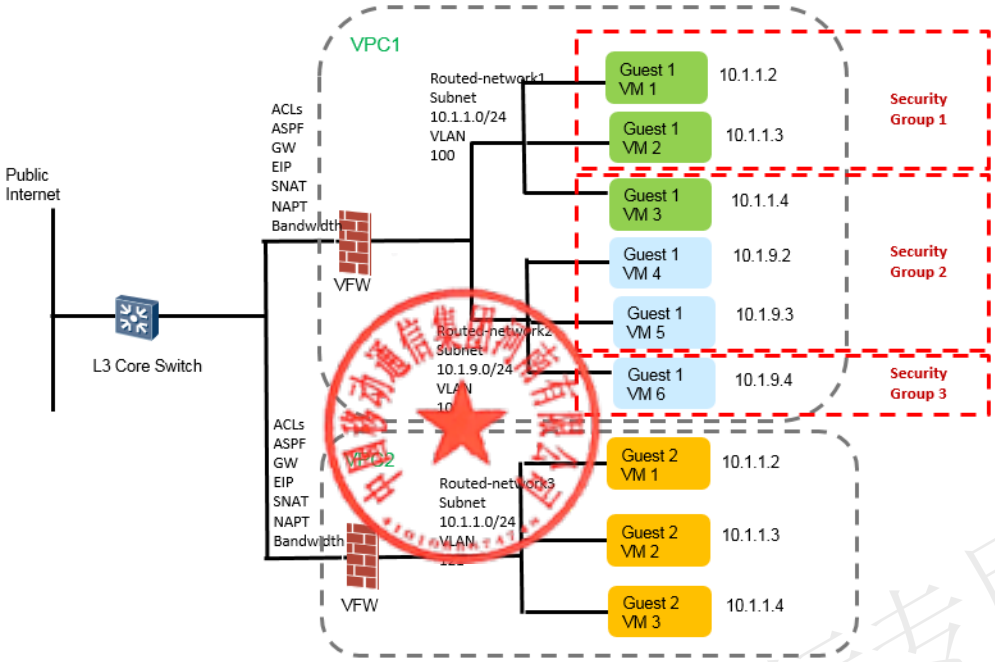
虚拟机可以加入安全组，安全组用来实现组内和组间的访问控制，加强虚拟机的安全保护，实现 VPC 内部的网络隔离。安全组通过配置安全规则来控制云主机网络消息的流入流出，只允许授权的消息通过。

系统存在一个默认安全组(default)，当项目管理员创建虚机不指定安全组的时候，系统会自动分配默认的安全组。管理员可以创建自定义的安全组，可以在安全组中定义各种访问规则，当创建一个新的安全组时默认有以下几条规则：

- 允许 IPv4 出方向访问；
- 不允许 IPv4 入方向访问；
- 同一个安全组成员可以互相访问；
- 不同安全组成员不可以互相访问；

安全组默认的一个规则是 Drop，当报文在一个安全组内不能匹配任何规则时，此报文会被丢弃。

公共资源交易平台招标专用



3.2.4.3.22 网络 ACL

网络 ACL（NetACL）是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。网络 ACL 与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络 ACL。安全组对弹性云服务器进行防护，网络 ACL 对子网进行防护，两者结合起来，可以实现更精细、更复杂的安全访问控制。

NetACL 支持与子网绑定，一个 NetACL 支持和多个子网绑定，一个子网不能同时加入两个 NetACL。

- 支持配置五元组。
- 支持一个防火墙实例关联多个 VPC。
- 防火墙与安全组差异对比

对比项	安全组	网络 ACL
防护对象	弹性云服务器级别操作	子网级别操作
配置策	仅支持允许策略	支持允许、拒绝策略

公共资源交易平台投标专用

对比项	安全组	网络 ACL
略		
优先级	多个规则冲突，取其并集生效。	多个规则冲突，优先级高的规则优先生效。
应用操作	创建弹性云服务器默认必须选择安全组，默认安全组自动应用到弹性云服务器	创建子网没有网络 ACL 选项，必须创建网络 ACL、添加关联子网、添加出入规则，并启用网络 ACL，才可应用到关联子网及子网下的弹性云服务器
报文组	仅支持报文三元组（即协议、端口和对端地址）过滤	支持报文五元组（即协议、源端口、目的端口、源地址和目的地址）过滤

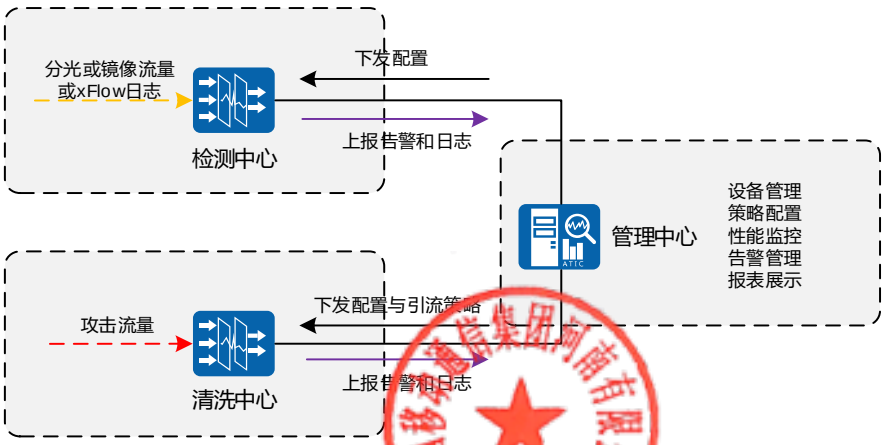
3.2.4.3.23 AntiDDos

Anti-DDoS流量清洗（以下简称Anti-DDoS）为公网IP提供四到七层的DDoS攻击防护和攻击实时告警通知。同时，Anti-DDoS可以提升用户带宽利用率，确保用户业务稳定运行。

AntiDDoS 通过对互联网访问公网 IP 的业务流量进行实时监测，及时发现异常 DDoS 攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时，Anti-DDoS 为用户生成监控报表，清晰展示网络流量的安全状况。

Anti-DDoS解决方案由华为自主研发的AntiDDoS和管理中心组成。其中AntiDDoS包含检测中心和清洗中心两部分，所以整个方案包括检测中心、清洗中心和管理中心三大部分。

公共资源交易平台技术专用
AE2C19CEC776161E1A62A8BC88EA14DB9



- **检测中心**

检测中心负责对流量进行检测，发现异常后上报管理中心，由管理中心下发引流策略至清洗中心进行引流清洗。检测中心的检测技术主要分为两种，一是基于Netflow的流量检测技术，二是基于应用的逐包检测技术，前者仅能检测大流量攻击，后者不仅能检测出大流量攻击还能够检测出小流量攻击和应用层攻击。

- **清洗中心**

清洗中心主要根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。清洗中心提供多种DDoS流量清洗手段，可以准确识别正常流量，清洗各类异常流量，包括流量型攻击、应用层攻击、扫描窥探型攻击及畸形包攻击。清洗中心同时具备检测中心的功能，当业务对检测清洗性能要求较低时可只部署清洗中心。

- **管理中心**

管理中心，负责检测中心和清洗中心的统一管理，是Anti-DDoS解决方案的管理中枢。提供设备管理、策略管理、性能管理、告警管理、报表管理等功能。

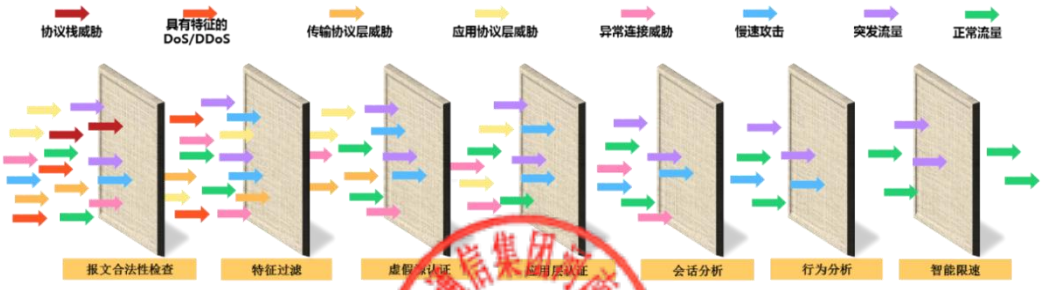
- **功能介绍**

手术刀式多层防范机制

移动清洗系统提供了逐层防范机制，使用报文合法性检查，特征过滤，虚假源认证，应用层认证，会话分析，行为分析，智能限速多种防范技术对流量进行层层筛选，保证攻击流量能够被相应算法识别并丢弃。其强大的防范机制

公共资源交易平台技术专用

可以灵活应对当前多变的DDoS攻击现状，为服务器提供100%的安全保证。



报文合法性检查

Anti-DDoS系统能够针对网络中的报文合法性做检查，针对违反RFC等协议标准的报文将直接丢弃，避免其可能对服务器造成的性能损耗。同时设备配备的强大DoS防范功能可以轻松应对LAND，Fraggle等常见传输层畸形包攻击，为服务器提供第一层安全保障。用于防范：Smurf攻击，Land攻击，Fraggle攻击，IP分片报文攻击，IP欺骗攻击，Ping of Death攻击， TCP报文标志位攻击，Teardrop攻击，WinNuke攻击。

特征过滤

基于大部分DDoS攻击均具有固定特征这个特点，移动开发了强大的特征过滤功能，能够针对源IP，协议，端口，负载，应用协议特定字段等信息进行匹配和过滤，实现对网络流量的灵活控制。同时搭配移动自研的动态指纹发现技术和抓包文件指纹自提取技术，减少了管理员手工介入防范的工作量，提高了应急响应效率。

利用特征过滤功能，移动Anti-DDoS系统集成了部分僵木蠕防范功能，用以防范经常伴随DDoS攻击出现的各种入侵，后门，远程控制行为。使用移动安全能力中心发布的特征库可以针对100+种流行的网络攻击进行防护。如UDP Flood、UDP类反射放大攻击（包括DNS反射放大，NTP反射放大等）。

虚假源认证

Anti-DDoS系统支持众多源认证算法，既包括syn cookie等业界通用防范算法，也包含了源IP信誉算法等一批具有移动自主知识产权的验证算法。清洗设备可以应用这些算法轻易的将虚假主机和正常访问客户区分开，有效避免屏蔽大量的虚假源IP攻击，形成源认证防范的第一道屏障。用于防范虚假源发起的

SYN Flood。

应用层认证

对于使用僵尸主机自身IP发起的攻击行为，移动提供大量的独特算法通过对应用层交互行为的检查来有效区分僵尸主机和正常访问客户，完成对正常用户的认证工作。同时搭配终端识别技术，可以获取客户端的详细信息，并根据不同客户端对应用协议的支持情况分别使用独立算法，有效降低了流量清洗出现误判的几率。用于防范虚假源或僵尸工具发起的DNS Query Flood、DNS Reply Flood、HTTP get/post Flood、HTTPS Flood、SIP Flood。

会话分析

移动清洗中心能够通过监控网络流量的实时信息，并记录于清洗系统专有的会话中。通过会话检测可有效防范TCP类异常会话攻击如慢速攻击、重传攻击、慢启动攻击，亦可有效防范DNS缓存投毒攻击、DNS反射攻击。在应用层DDoS攻击发展迅速的今天，会话分析将是一种重要的防范技术。用于防范如ACK Flood、FIN/RST Flood、TCP连接耗尽攻击、socktress、重传攻击、DNS Cache Poisoning、SSL-DoS/SSL-DDoS、 HTTP slow headers/post attack。

行为分析

僵尸网络的攻击行为和正常用户的访问行为存在很大差别，主要表现在正常用户的访问具有突发性及无序性，而僵尸网络的攻击属于机器人攻击，频率恒定，或者访问的资源基本保持不变，或者TCP流量比率异常，或者攻击报文负载不变，移动清洗设备能够采用指纹学习或访问频率行为学习来防范该类攻击。用于防范CC攻击、慢速SYN Flood。

智能限速

Anti-DDoS系统能够智能的对网络中的IP流量和应用层流量进行分析，对于流量大于特定值的流量能够实施基于源IP，目的IP，报文类型，特定字段的限速。以实现对整网流量的可控，可限，保证后端服务器在大量正常流量冲击下任能提供服务。

灵活的部署

移动Anti-DDoS产品提供强大的路由和转发功能，保证了在复杂的客户网络中总是能够合理的部署DDoS防护系统。

引流技术

移动提供业界最强大的BGP路由功能，在Anti-DDoS方案中可以灵活的针对流量进行牵引，并通过路由策略准确的控制路由发布。而BGP邻居安全认证技术则保证了BGP连接的安全。同时移动也提供了策略路由，IGP等其它的引流技术以供特定场景使用。另外，移动引入了动态引流，静态引流，手工引流等多种引流方式，提供流量牵引的灵活性。

回注技术

在做旁路部署时，流量如何回注一直是Anti-DDoS系统部署的难题。为了应对此问题，移动Anti-DDoS清洗设备支持丰富的回注技术，包括MPLS，MPLS L3 VPN，GRE，802.1q，PBR。其中MPLS和MPLS L3 VPN能够应对复杂组网要求，其余技术针对网络边界防护能够提供有效支持。

高可靠

为了应对网络设备可能突发的故障问题，移动Anti-DDoS解决方案提供了一整套高可靠性技术。

方案级可靠性：

逐包检测+动态引流清洗：

通过分光/镜像复制一份流量到Anti-DDoS设备进行检测，发现异常后发送主机路由动态引流受攻击地址的流量到Anti-DDoS进行清洗。无论是检测中心、清洗中心、管理中心或者DDoS系统网元间的连接故障，都只会导致Anti-DDoS系统暂时无法提供DDoS防护能力，管理员可以根据Anti-DDoS相关的故障信息快速修复故障，期间不会对现网业务造成任何影响。

Netflow检测+动态引流清洗：

路由器/交换机发送流量汇总信息（Netflow）给Netflow分析器（GenieATM），Netflow分析器汇总各个路由器/交换机的Netflow信息，发现攻击后发送syslog日志给ATIC，ATIC启动引流清洗。无论是检测中心、清洗中

心、管理中心或者DDoS系统网元间的连接故障，都只会导致Anti-DDoS系统暂时无法提供DDoS防护能力，管理员可以根据Anti-DDoS相关的故障信息快速修复故障，期间不会对现网业务造成任何影响。

低误判

移动清洗系统为降低清洗对网络影响，提出了基于业务的精细化清洗思路。所有清洗活动以目的 IP，端口和协议为最小粒度，保证其它未受攻击业务直接转发。针对 Anti-DDoS 产品可能出现的误判和错判情况进行了算法改进，提出了包括 DNS 被动源认证等多种改进算法，保证正常业务不会因为清洗而出现中断。针对目前终端设备对应用协议栈支持程度不一这种情况，移动公司提出了终端识别技术等一批终端鉴别技术，针对不同终端和应用将分别使用独立的防范算法，进一步降低了 Anti-DDoS 误判的可能性。

3.2.4.3.24 网闸

网闸，又称为物理隔离网闸，网闸主要是通过在网络模型的各层的断开，例如物理层断开、链路层断开、TCP/IP 协议隔离和应用协议隔离，因此，网闸从逻辑上隔离、阻断了对内网具有潜在攻击可能的一切网络连接，使外部攻击者无法直接入侵、攻击或破坏内网，保障了内部主机的安全。

网闸就是要解决目前网络安全存在的下述问题。

（1）对操作系统的依赖，而操作系统可能有漏洞，存在被攻击的风险；

（2）对 TCP/IP 协议的依赖，而 TCP/IP 协议有漏洞；

（3）解决通信连接的问题，内网和外网直接连接，存在基于通信的攻击；

（4）应用协议的漏洞，如非法的命令和指令等。

3.2.4.4 密码应用安全

3.2.4.4.1 云平台密码应用安全方案

3.2.4.4.1.1 方案概述

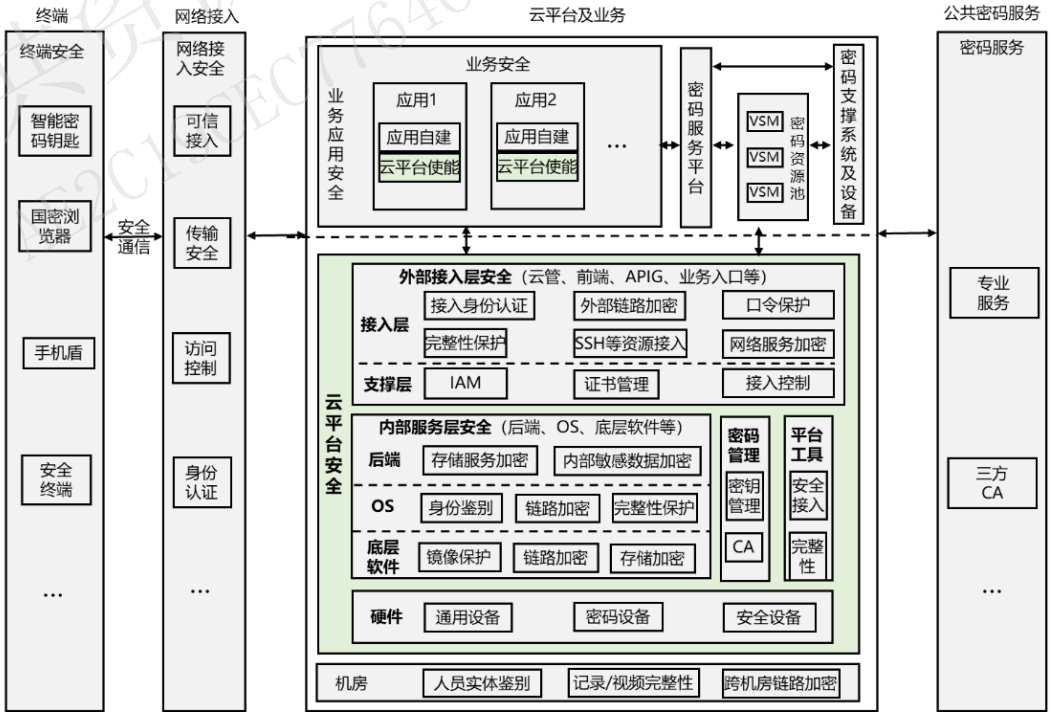
密码技术作为网络与信息安全保障的核心技术和基础支撑，在身份认证、信息加密、安全隔离、完整性保护和操作抗抵赖等方面发挥着不可替代的作用。

2019 年 10 月 26 日，十三届全国人大常委会第十四次会议通过《中华人民共

和国密码法》，于 2020 年 1 月 1 日起正式实施。密码法的出台，为密码科技实现跨越式发展、密码科技创新再上新台阶提供了宝贵的战略机遇和发展契机。随着云计算技术的深入发展和应用，各行各业纷纷上云，但云环境面临传统安全边界消逝、虚拟环境数据安全等更加严峻的安全挑战，如何用密码技术保障云环境安全是研究的一个焦点。如何合规、正确、有效的在云平台内使用商用密码，充分发挥商用密码在保障关键基础设施安全的核心技术和基础支撑作用，关乎网络空间安全、用户隐私。

为满足《中华人民共和国密码法》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，及政务、金融、信创等多行业领域客户关键信息基础设施商用密码防护需求，华为云在云平台内落地商用密码，构建完善的密码防护体系，在云平台内生能力上做到 “SM inside”，保障交付中国区重点行业客户的云平台安全、合规，同步提升云平台自身内生安全防护，实现机密性、完整性、真实性、不可否认等安全目标。

结合重点项目密码应用需求，密码应用总体架构包括四部分内容：终端安全密码应用、网络接入安全密码应用、云平台及业务密码应用、云安全管理密码应用四部分。在云平台及业务密码应用部分，分为云平台安全密码应用、业务安全密码应用、机房安全密码应用。



密码应用技术架构

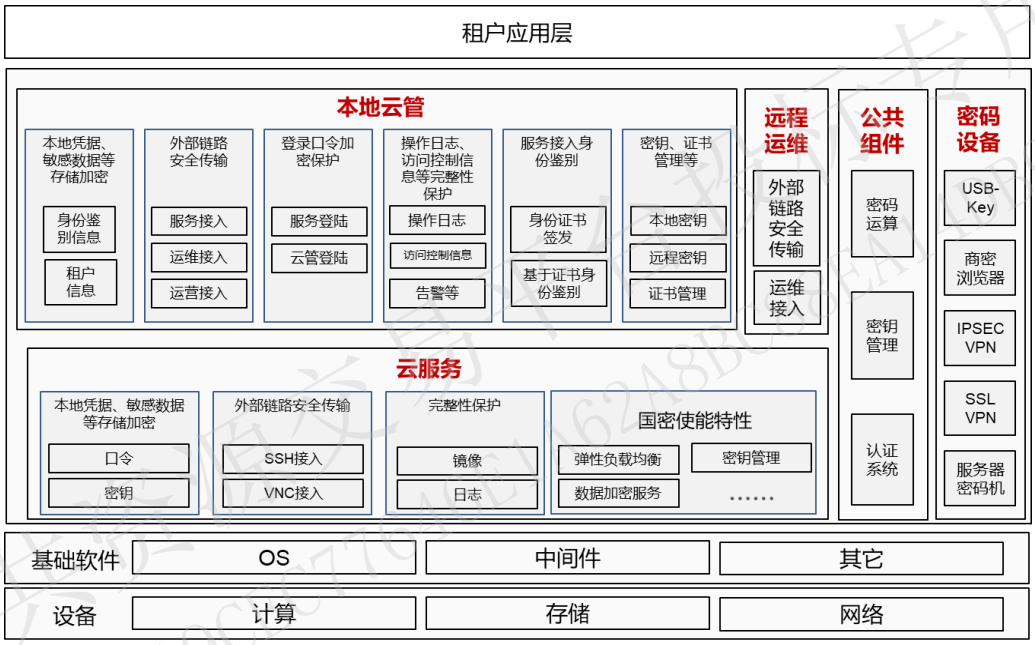
终端安全，主要包含商密浏览器、智能密码钥匙、客户端等终端接入所需身份鉴别、链路防护的组件；

网络接入部分，主要进行可信接入认证、链路安全传输、访问控制等；

云平台和业务部分，需要实现对外部接入云平台基于数字证书的用户身份鉴别、传输链路安全、口令保护等，同时需解决服务内部重要数据的完整性保护、存储加密、密钥管理、证书管理等；

密码服务部分，主要包含对接通过网络提供服务的互联网 CA、密码服务等。

具体到云平台内部，主要进行如下功能适配改造：



云平台密码改造架构

具体方案层面，基于自研公共密码组件，集成满足二级密码模块要求的三方密码设备，对云服务、云管平台、远程运维等进程多方面改造，在云平台内落地商用 SM 密码，构建完善的密码防护体系，同步提升云平台自身内生安全防护。云平台内主要改造点如下：

1. 平台内存储的本地凭据、敏感数据存储加密，主要涉及云管、各服务等各类组件；

2. 服务接入、运维接入、VNC 接入等外部链路传输安全加密，支持商密 SM2 双证书体系，主要涉及运维接入 OC 及 ServiceOM、运营接入 Console、VNC 等；

3. 服务、云管、OS 等登录口令加密保护，主要涉及 IAM、ManageOne OC、

OS 等；

4. 镜像、日志等重要数据完整性保护，主要涉及 IMS、ECS、ServiceOM、MangeOne OC 等；

5. 服务、云管接入支持基于证书的身份鉴别，支持商密 SM2 双证书体系，主要涉及 MangeOne SC、OC 等；

6. 支持统一的密钥、证书管理，主要涉及 KMS、ManageOne OC 等；

同时，关键云服务 ELB、KMS、DEW 等支持商密能力，使能租户业务应用商密改造。

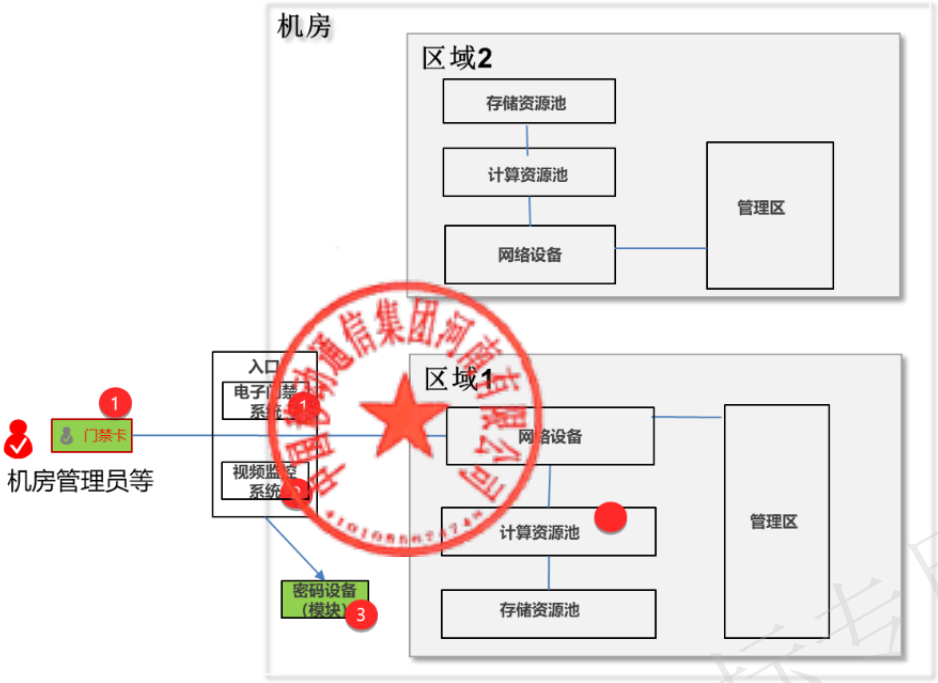
3.2.4.4.1.2 物理和环境安全

物理核环境安全需要机房提供方提供，推荐方案如下：

物理和环境安全总体要求应采用密码技术对重要场所、监控设备等物理访问进行控制；采用密码技术对物理访问控制记录、监控信息等物理和环境的敏感信息数据实施完整性保护；基于总体要求采用数据完整性保护机制保证访问控制记录、监控信息等物理环境的敏感信息的完整性。

在系统环境监控区部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，使用 HMAC-SM3 技术对电子门禁系统进出记录和视频安防系统视频记录等数据进行完整性保护，其中 HMAC-SM3 密钥由环境监控区服务器密码机生成，存储在服务器密码机中，不涉及密钥分发、导入与导出，密钥的备份与恢复、归档和销毁由密码设备管理员负责。物理和环境安全层面使用的密码算法、密码技术、密钥。

公共资源交易平台技标专用
AE2C15CE0276161A624B0C88EA1...



机房密码改造架构

① 人员身份鉴别:基于门禁系统，进行物理访问的身份鉴别，保证机房及重要区域进入人员身份真实性；

②门禁记录日志完整性保护接入：对门禁记录日志文件进行数据完整性保护。

③视频安防文件完整性保护接入：对机房视频安防文件进行数据完整性保护，它通过对接服务器密码机等实现数据完整性保护。

④对接服务器密码机等进行文件完整性保护：为降低应用系统或设备产生的重要数据、敏感信息等结构化数据被截获、篡改、监听等风险，保证数据的完整性，需要对重要数据信息进行完整性保护，可对接服务器密码机 HSM 等，对结构化数据完整性保护。

建议改造清单：

编号	分类	相关产品	数量（台套）	主要功能
1	物理和环境	门禁系统	1	使用商密算法进行密钥分散，实现门禁卡的“一卡一密”，并基于商密 算法对人员身份进行实体鉴别

公共资源交易平台投标专用

编号	分类	相关产品	数量（台套）	主要功能
2		视频安防系统	1	监控人员进出、活动行为等，支持对视频安防系统视频记录等数据进行完整性保护
3		服务器密码机	2	对电子门禁系统进出记录和视频安防系统视频记录等数据进行完整性保护

机房密码改造推荐清单

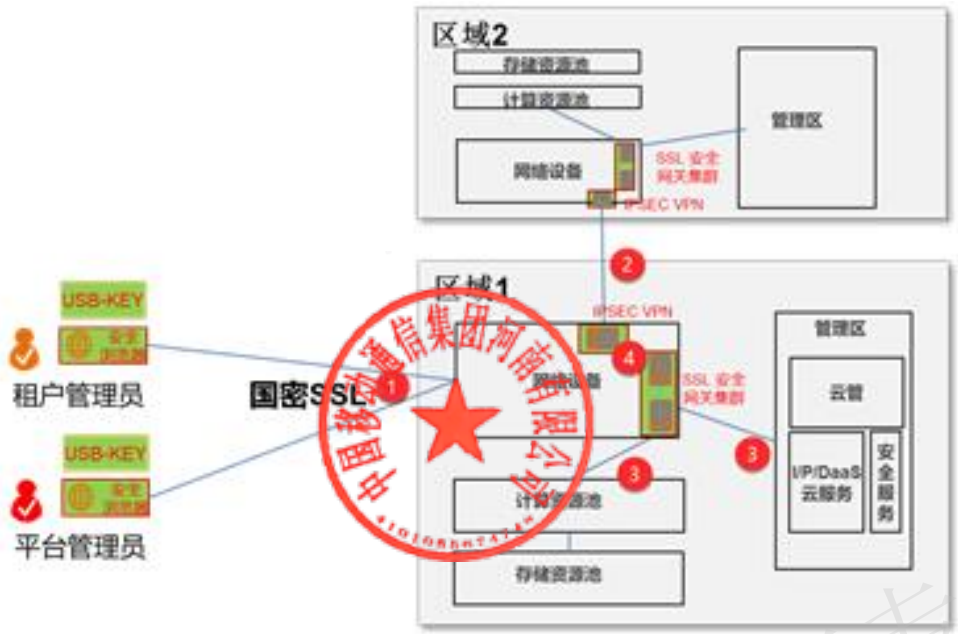
3.2.4.4.1.3 网络和通信安全

网络和通信安全部分，主要通过集成合规的密码设备（满足商密模块 2 级要求）完成。不涉及云平台内部改造，涉及云平台组网支持。

网络和通信安全的总体要求总则：采用密码技术对通信的双方身份进行认证；采用密码技术保证通信过程中数据的完整性;采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；采用密码技术保证网络边界访问控制信；采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。

为满足网络和通信安全的总体要求需要通过 IPSec VPN、 SSLVPN、USBKey 配合商密安全浏览器构建虚拟专用通道来保证对网络和通信部分的安全：

公共资源交易平台投标专用



网络和通信安全架构图

① 云平台接入侧部署 SSL VPN 网关，云平台管理员和租户通过安全浏览器和 SSL VPN 网关完成通信双方的身份鉴别、通信数据的完整性保护和机密性保护，利用 SSL VPN 网关本身的机制完成对于访问控制信息完整性的保护。

② 云平台利用 IPSec VPN 完成机房之间的通信双方的身份鉴别、通信数据的完整件和机密性保护。

③云平台管理员通过 SSL VPN 网关、堡垒机对物理机和虚拟机进行集中管理。

④网络边界访问控制信息的完整性，采用 SSL VPN 网关等设备对网络边界访问控制信息基于 HMAC-SM3 进行完整性保护。

建议密码产品清单

编号	分类	相关产品	数量（台套）	主要功能
1	网络和通信安全	SSLVPN安全网关	2	配套安全浏览器、移动终端密码模块等，在云平台与云平台管理员、用户之间建立安全通道。兼具接入认证相关功能。
2		IPSEC VPN设备	2 / 机房	IPSEC VPN用于机房之间建立安全通信通道；符合

公共资源交易平台投标专用

编号	分类	相关产品	数量（台套）	主要功能
				GM/T 0022-2014《IPSec VPN技术规范》、GM/T 0023-2014《IPSec VPN网关产规范》
3		安全浏览器	N（按需）	配合SSL VPN，在云平台与云平台管理员、租户之间建立安全通信通道
4		智能密码钥匙	N（按需）	存储云平台、租户管理员密钥对，配套本地套件包，用于云平台管理员、租户管理员登录服务器和云平台管理应用时的身份鉴别，以及与云平台管理应用之间进行安全通信

网络和通信安全密码设备清单

公共资源交易平台投标专用

3.2.4.4.1.4 设备和计算安全

设备与计算安全需采用密码技术对登录的用户进行身份鉴别，在本系统业务区 PC 端部署安全浏览器，并向系统管理员配发 USBKey，对登录设备（堡垒机、VPN 等设备）的用户进行身份鉴别，防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。

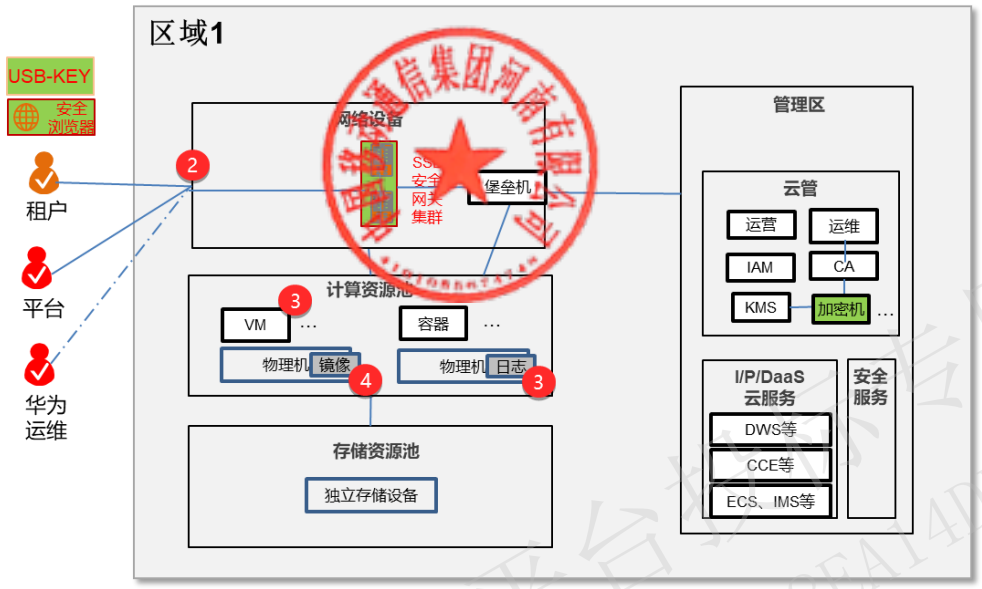
对设备的远程操作管理通过 VPN、VPN 综合安全网关等设备，建立安全的信息传输通道，实现管理过程中通信的机密性、完整性。

通过云密码服务管理平台的完整性功能，保证系统资源访问控制信息的完整性、对重要程序或文件进行完整性保护、对日志记录进行完整性保护。

通过云密码服务管理平台完整性保护功能，通过上传重要可执行程序的 Hmac

值或签名信息，以及软件的真实来源信息，在软件启动时调用接口对相关信息进行校验，实现对重要可执行程序进行完整性保护和来源真实性验证。

为满足设备和计算安全的总体要求，需要通过 SSH 协议、SSLVPN、商密浏览器、OS 完整性保护等，来保证对设备和计算部分的安全：



设备和计算安全机构图

① 身份鉴别：云平台运维管理员和租户接入物理机和虚拟机进行管理前，支持基于 SSH 等机制对用户进行身份鉴别。也在网关后部署堡垒机，对管理员接入身份进行认证鉴别；

② 远程管理安全通道：通过 SSL VPN 网关与安全浏览器间搭建的安全通信链路，完成对远程管理身份鉴别信息机密性的保护；

③ 系统资源访问控制信息、日志等完整性：云平台使用的通用服务器自身通过 OS 等改造，利用物理密码机或密码模块，采用 HMAC-SM3 算法对设备资源访问控制信息、日志等进行完整性保护；

④ 重要程序或文件完整性和来源真实性验证：云平台自身使用的通用服务器中重要程序或文件（包括虚拟机镜像模板等）在生成时利用数字签名进行完整性保护，使用或读取这些程序和文件时，进行验签以确认其完整性；

建议密码产品清单

公共资源交易平台系统专用

编号	功能点	相关组件	主要功能	备注
1	SSH登录	OS	支持SM2、RSA等非对称算法，对SSH链路接入进行加密保护	
2	OS口令加密保护	OS	对登录OS口令加密保护，支持商密SM3、SHA512等	
3	OS内重要数据完整性	OS	支持对OS内的系统资源访问控制信息、重要程序或文件完整性等进行完整性保护，支持SM3机制	
4	VNC登录	ECS等	支持对ECS虚拟机等VNC登陆时，链路加密防护，支持商密算法	
5	镜像完整性	IMS、ECS等	支持对公共镜像、私有镜像的完整性保护，支持商密算法	
6	软件程序完整性保护	HCSD、HCSU	安装升级、场景，基于RSA2048/3072/4096算法等，对软件包完整性进行校验	

设备和计算安全设备清单

（一）SSH 登录适配

提供 openssh 组件提供了对商密算法中 SM2/SM3/SM4 的支持，以支持用户登录时可以使用商密的系列算法，提供了涉及密钥交换、公钥认证、对称加密和完整性认证的系列商密算法登录配置。

（二）OS重要数据完整性适配

OS 口令支持 SM3 算法加密，也支持使用 SHA512。

（三）OS重要数据完整性

公共资源交易平台专用

Linux OS 入侵检测机制支持 SM3、SHA256、SHA512 等多种 Hash 加密方式，对文件内容生成摘要信息，并通过对比文件属性与摘要信息，以发现当前系统文件是否被恶意修改。OS 入侵检测机制商密改造是基于该机制的原有功能，在 Linux libgcryp 库合入商密 SM3 算法补丁，AIDE 做相关适配，以支持 AIDE 使用 SM3 hash 算法对文件内容进行摘要值计算。摘要值计算原理是根据文件内容作为输入，通过指定算法计算 hash 值，再通过 base64 编码生成摘要值。

（四）VNC登录适配

VNC 方式是 UI 界面提供的可远程登录弹性云服务器/裸金属服务器的能力，使用 https 协议对外提供服务。当前版本支持商密 SM 系列算法进行链路加密防护，支持商密浏览器进行访问。同时支持商密和国际兼容算法进行 vnc 登录。

（五）镜像完整性保护

镜像完整性是云平台提供的用户从注册镜像到发放弹性云服务器/裸金属服务器整个流程中，使用数字签名算法保证镜像在传输过程中的完整性，不被篡改。在镜像注册过程中，系统默认使用哈希算法（SHA256/SM3）计算镜像的 HASH 值，使用证书通过 HASH 值计算镜像的签名值，支持 RSA 和 SM2 算法。在发放弹性云服务器/裸金属服务器的过程中，会重新计算镜像的 HASH 值和签名值进行校验，以保证镜像的完整性。整个过程用户不需要额外进行操作。

3.2.4.4.1.5 应用和数据安全

应用和数据安全部分，主要通过云平台改造来满足，涉及云平台内云服务、云管、工具等改造。

在各个 Region，部署密码机，以集约化的方式为网络区中云平台服务、业务系统提供密码服务，满足云服务通过三级密码应用安全性评估需求。通过部署密码服务管理平台，实现密码服务、密码设备的统一管理，避免密码设备的重复投资。

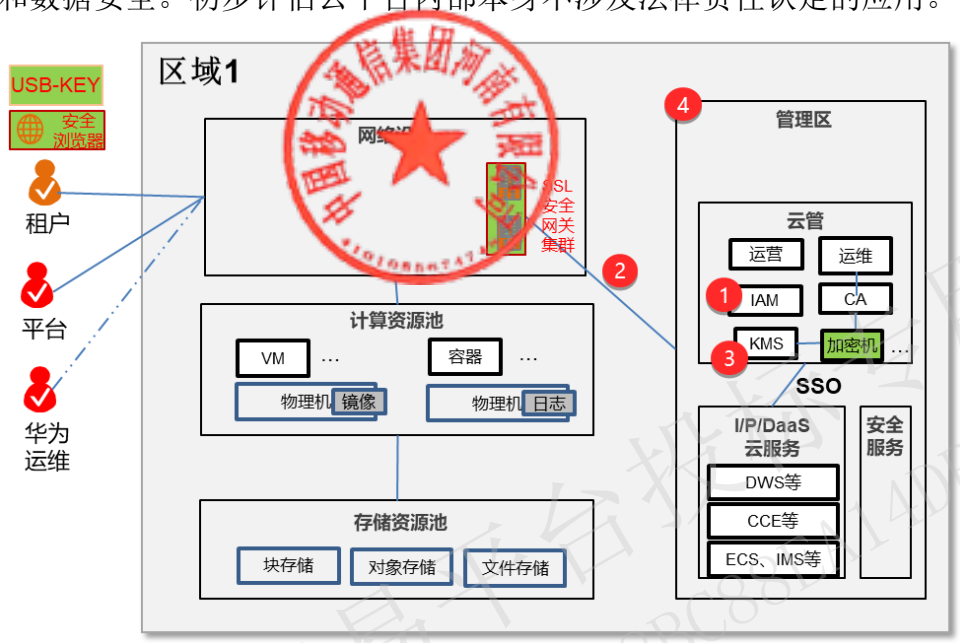
总体功能及要求包括：

1. 通过 USB key 等设备或软件模块，配合后台设备系统，满足应用系统采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性的需求。

2. 通过云平台的密码模块对接硬件 HSM，实现信息系统应用的操作日志、访问控制信息等的完整性保护。

3. 服务调用软件密码模块和硬件密码机等密码设备，实现重要数据在传输过程和存储过程中的机密性和完整性。

应用和数据安全部分，需要在云管及云服务应用层对管理员身份进行鉴别，并保障重要数据的传输、存储安全，同时保护访问控制信息等完整性，来实现核心应用和数据安全。初步评估云平台内部本身不涉及法律责任认定的应用。



应用和数据安全架构图

① 身份鉴别：云平台管理员和租户接入云平台管理平台和云服务应用前，需要通过 IAM 进行身份鉴别（对接 CA 支持商密证书的签发、验证，CA 对接硬件加密机）。身份鉴别平台对云平台管理员/租户的身份鉴别方式为智能密码钥匙证书 + PIN 码的双因素身份鉴别；

② 数据传输安全：平台管理员/租户和云平台管理应用之间的数据传输，平台管理员/租户管理员，在商密浏览器和云服务间构建 Https 通道。结合网络层链路防护，保护传输数据机密性与完整性。

③ 访问控制信息：云平台云管服务、云服务等自身利用物理密码机或密码模块，采用 HMAC-SM3 对其 IAM 访问控制策略等进行完整性保护；

④ 重要数据存储安全：云平台云管等各服务内部的敏感数据、鉴别信息、操作日志、租户信息等，调用 KMS（对接物理密码机）或内置密码模块，采用 SM4 算法对关键数据进行机密性保护，然后存放在数据库、磁盘中；2）支持使用 HMAC-SM3 算法对操作日志等关键数据进行完整性保护。

⑤ 不可否认性：不涉及（云平台内不涉及法律责任认定的应用）。

编号	分类	相关产品	数量（台/套）	主要功能
1	应用和数据安全	CA	1/ManageOne	进行商密证书的签发、生命周期管理等。

应用和数据安全密产品

（一）基于数字证书身份认证

云管平台管理员、租户用户接入运管平台和云服务 console 需通过运管平台身份认证，云管平台身份认证支持多种登录认证方式：

1）基于商密证书的 USB-Key、PIN 码双因子认证：用户使用 USB-Key 访问云管平台的登录页面，从 USB-Key 中选择用户证书，运管平台校验证书和设备应用 PIN 码，通过证书、PIN 码双因子认证，成功后方可登录云运管平台和云服务 console。

2）用户名/口令认证，支持扩展短信/邮箱验证码等双因子认证。

（二）OC 运维通道安全接入

OC 是云管平台运维中心，运维 Portal 提供云服务整体运维入口。管理员通过商密浏览器接入 OC，HIROERService 服务作为服务端是外部流量的统一入口，端口支持 tls 协议，兼容支持商密算法加密，并提供了鉴权，路由转发，限流等一系列 service mesh 能力。

（三）ServiceOM 运维通道安全接入

ServiceOM 是云服务的运维 Portal，提供 IaaS 的整体运维能力。浏览器发起对 ServiceOM 请求，会经过 Nginx 然后到达服务组件 tomcat，商密能力主要由 nginx 提供。

管理员通过商密浏览器接入 ServiceOM， ServiceOM 的 TLS 链路提供了兼容支持商密算法的加密防护。TLS 加密套件除了符合安全要求的国际算法套件外，新增 ECC-SM4-SM3、ECDHE-SM4-SM3 国密算法套件。

（四）服务 Console 接入功能

租户/管理员通过商密浏览器接入云服务 Console， TLS 链路提供了兼容支持商密算法的加密防护。TLS 加密套件除了符合安全要求的国际算法套件外，新

公共资源交易平台技术专用

增 ECC-SM4-SM3、ECDHE-SM4-SM3 国密算法套件。

（五）API 接入安全通道

华为云 Stack 解决方案 API 均通过 API 网关对外提供服务。当用户需要基于华为云 Stack 开发应用或云平台时，可以直接调用 API 网关上开放的 API。华为云 Stack 解决方案 API 分认证、运维、运营、IaaS、PaaS、DaaS、BR&DR（灾备）等几部分。

从云外调用 API 过来的流量（https/external）要支持国密算法，在 APIG 转发时做商密 https 的支持。

（六）灾备安全接入功能

1.eBackup:主要应用于用户浏览器侧访问备份 portal 页面时进行安全通信，进行添加受保护环境、添加存储单元、安全选项配置等操作。备份 ebakcup 对外提供 portal 界面，通过用户名密码登录，采用 https 通信，涉及到的 nginx 支持国密，配套支持国密的浏览器，实现传输通道的安全接入。

2.eReplication:主要应用于用户浏览器侧访问容灾 portal 页面时进行安全通信，进行计划性迁移、故障恢复、重保护等操作。容灾 eReplication 对外提供 portal 界面，可以通过两种方式登录该界面，一是用户名密码，二是通过 ManageOne 的 SSO 单点登录。浏览器发起访问 portal 界面请求，会经过 Nginx、tomcat，最终到达 eReplication-server 组件，如下图所示。浏览器发起的 https 请求，与 nginx 组件协商安全通信算法套，所以是由 Nginx 支持国密算法来实现传输通道的安全接入。

（七）云服务内敏感数据加密

云服务内部涉及本地配置信息（一般为口令、密钥等）、敏感业务数据（用户隐私信息如邮箱、手机号等）需要加密保护。云平台内部各云服务、云管等组件，对本地配置信息、敏感业务数据等进行存储加密，支持商密算法

（八）云 OS 内敏感数据加密

EulerOS Virtual 虚拟化组件提供了对 SM 系列商密算法的支持，并通过 KMC 模块对密钥进行管理。支持用户在需要时，可以通过调用 EulerOS Virtual 提供接口切换虚拟化组件使用的加密算法。EulerOS Virtual 安装部署完成，通过 osfilecheck -s compatible 配置 aide 的文件校验码或哈希值加密算法为商密

SM3 后，用户执行 osfilecheck -i，初始化数据库，此时通过商密 SM3 去生成文件的校验码或哈希值存于数据库中，当用户下次去执行 osfilecheck -c 时，aide 会再次通过商密 SM3 计算文件的校验码或哈希值，并与数据库中对应文件的校验值或哈希值进行对比，有差异则说明文件被修改，否则文件未被修改。

（九）操作日志完整性保护

ManageOne 租户操作日志提供了统一的租户面操作日志审计功能，记录租户在使用云服务时的操作记录，帮助管理员了解系统运行状况，了解用户行为，排查系统故障，识别并消除安全威胁。由于租户操作日志的重要性，所有需要对日志的完整性进行保护，防止恶意篡改导致审计问题。对租户操作日志记录计算 HMAC 进行完整性保护，包括：

- 对租户的操作行为记录日志时，对全量日志字段信息生成HMAC值，并保存到数据库；
- 用户查询日志时，针对过滤出的日志校验HMAC，在操作日志查询结果中展示日志校验结果，是否被篡改，如发现日志被篡改，查询结果中提示用户；
- 后台定时验签三天内的日志，校验日志是否被篡改、删除或插入，并记录系统日志；
- 后台提供独立验签工具，校验日志是否被篡改、删除或插入，并给出校验结果并记录系统日志；
- 日志完整性支持对历史日志记录进行HMAC签名处理，从启用该能力时间点最近30天内的日志，最多100万条做HMAC签名。

（十）服务口令登录保护

用户使用云管平台运维中心、服务中心，首先使用预置账户/口令登录后，创建新用户，为用户设置密码或者申请证书完成 USB-Key 制证。用户使用用户名/口令或者 USB-Key、PIN 码登录云管平台运维中心、服务中心。云管平台运维中心、服务中心支持用户名/口令，短信/邮件验证码的双因子认证，同时支持 USB-Key、PIN 码双因子认证。云管平台对口令做单向哈希保护，在国产密码算法模式下支持 PBKDF2-HMAC-SM3 加密保护。

公共资源交易平台投标专用

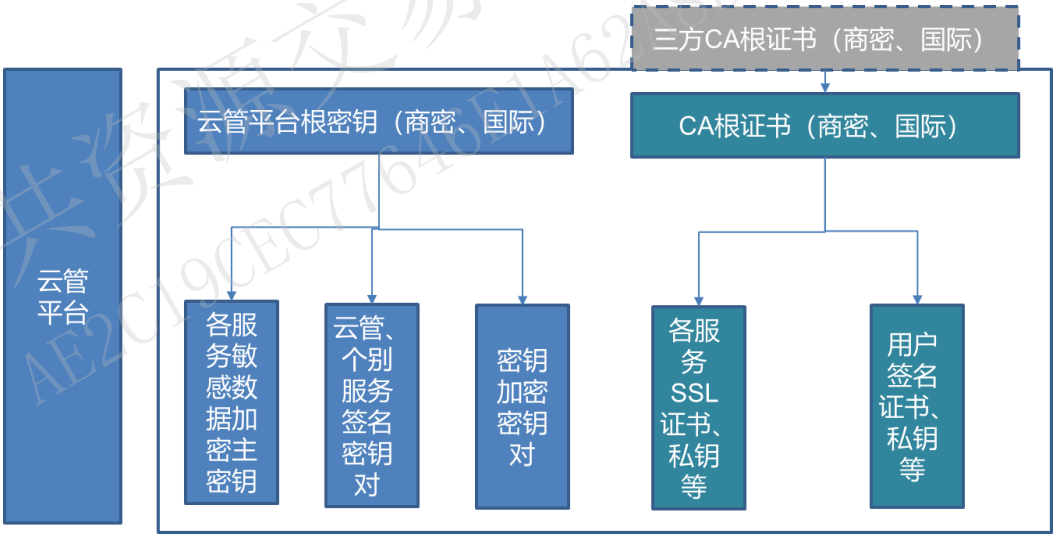
3.2.4.4.1.6 秘钥管理

云平台本身的密钥体系可以分为云平台管理密钥和云上应用层两层密钥。密钥数据必须密文存储且与云平台其他数据存储分离；确保用户在云平台中使用密钥时，处于独立安全环境中；具有密钥隔离手段，用户一旦销毁密钥，密钥管理系统必须对密钥及时销毁且不可恢复。

密钥管理系统是基于密码资源池基础设施，通过虚拟化镜像部署到 ECS 虚拟服务器，为云平台及云上业务系统提供密钥托管相关的支持活动，主要功能是密钥托管、密钥安全隔离和存储、密钥安全访问、密钥的策略控制、基于托管密钥的简单加解密、密钥使用的日志记录、密钥高可靠等。密钥服务包括密钥生成、分发、存储、更新、导入、导出、备份、恢复，主要借助硬件密码模块 HSM 生成密钥，密钥不得以明文形式出现在云密钥管理服务之外，确保密钥安全。

非对称密钥的管理主要通过证书管理系统等完成，对各类人员签名证书、服务 SSL 证书等进行统一生成、分发、更新、导入、备份、吊销、到期提醒等。

云平台密钥管理总体结构如下所示，主要涉及 KMS、证书管理、CA 等公共组件。



秘钥管理架构图

1） 云管平台主密钥对以下密钥进行保护：

各服务的敏感数据加密密钥主要用作重要数据的加密，以及重要数据的完整性保护。

云管、个别服务的数字签名密钥对主要为实现操作与传输文件的不可否任性和完整性。

密钥加密密钥对主要对数据传输中数据交换密钥进行机密性与完整性保护。

2）三方或自建 CA 对各类证书进行保护：

各服务的 SSL 证书、私钥等，由 CA 生成分发到各服务，进行安全数据传输及对称密钥交换等；

各用户的签名证书、加密私钥等等，有 CA 生产经云管分发到个用户，一般在智能密码钥匙等中持久化保存。

编号	功能点	相关组件	主要功能	备注
1	密钥管理	KMS	支持AES、SM4、SM2、RSA等对称、非对称算法密钥生命周期管理，支持对接满足二级密码模块认证的HSM	
2	证书管理	OC	支持对证书的生命周期管理，支持RSA、SM2证书等	
3	CA对接	OC	支持集成LiteCA和三方CA，提供证书签发基本能力，支持签发RSA、SM2等算法证书	

秘钥管理密码产品

（一）秘钥管理

密钥管理服务提供统一的密钥管理功能，支持对接满足二级密码模块认证的 HSM，各云服务通过对接 KMS 及 HSM 进行根密钥保护。支持对称、非对称密钥的管理，支持常见算法 RSA、SM2、AES、SM4 等。

- 租户、云服务密钥的统一管理：租户/服务主密钥生命周期管理、数据密钥管理
- 主密钥全生命周期管理：创建、启用、禁用、删除、轮转、授权、别名、修改描述、导入、查询、搜索、标签管理等；
- 数据密钥管理：创建、加密、解密；
- 根密钥保护：基于硬件HSM根密钥保护；

（二）证书管理

公共资源交易平台招标专用

证书管理的应用场景主要包括证书查看、证书替换和证书吊销。证书管理下发的证书、私钥由对接的 CA 服务器颁发或者用户在证书管理界面导入，证书管理负责分发给对应更新的部件。

证书管理的应用场景主要包括证书查看、证书替换和证书吊销。证书管理下发的证书、私钥由对接的 CA 服务器颁发或者用户在证书管理界面导入，证书管理负责分发给对应更新的部件。

证书过期时，运维人员可根据是否需要配置 CA，选择更新或导入的操作维护证书。

对于不再需要的证书，运维人员可下发证书吊销信息，使该证书功能将失效。

1. 解决方案各部件将涉及的证书通过 ManageOne 统一注册到证书管理功能中，运维人员通过证书管理界面运维各证书。

2. 在对证书进行维护前，需要首先配置与系统对接的 CA 服务器的参数，完成与 CA 服务器的对接。

3. 其次需配置证书规格，包括证书的格式、生成密钥对的算法、生成密钥对的长度以及证书有效期。

4. 在维护过程中，运维人员可对证书进行查看、更新、导入和吊销的操作。

（三）CA 对接

CA 对接用于对接 CA 服务器，对接后用于证书管理申请证书。在国密场景下，用户管理也通过对接的 CA 服务器申请 USB-Key 证书。CA 服务器对接使用 CMPv2 协议与 CA 服务器交互。CRL 服务器对接使用 FTP、Ldap 协议获取最新 CRL 文件。

3.2.4.4.1.7 安全合规性分析

根据华为云商密支持技术方案，结合密码应用标准，对标 3 级系统进行安全域合规自查，物理和环境、网络和通信层技术符合度自评（三级）如下。

No	分类	具体指标	要求	技术手段	符合情况	备注
1	物理和环境	身份鉴别	宜	门禁卡 + 电子门禁系统，并基于 商密算法实现门禁卡的	符合	正常由机房建

No	分类	具体指标	要求	技术手段	符合情况	备注
	安全（10）			“一卡一密”，对人员身份进行实体鉴别		设/管理方改造完成
2		电子门禁记录数据存储完整性	宜	使用 HMAC-SM3 技术对电子门禁系统进出记录、视频安防系统视频记录等数据进行完整性保护，其中 密钥由密码设备（模块）生成，存储在密码设备（模块）中	符合	
3		视频安防记录数据存储完整性	宜		符合	
4		密码服务	应	使用符合法律法规的相关要求并经商用密码认证机构认证合格的密码服务	符合	
5		密码产品	二级及以上	使用的密码产品达到 GB/T 37092 二级及以上安全要求	符合	
6	网络和通信安全（15）	身份鉴别	应	云平台接入侧部署SSL VPN网关，云平台管理员和租户通过安全浏览器浏览器和SSL VPN 网关完成通信双方的身份鉴别	符合	集成SSL VPN网关和IPSEC

公共资源交易平台技术专用
AE2C19CEC77646E1A62BBC88EA14DB9

No	分类	具体指标	要求	技术手段	符合情况	备注
7		通信报文完整性	宜	平台接入侧部署SSL VPN网关，云平台管理员和租户通过安	符合	VPN设备满足
8		敏感字段或通信报文的机密性	应	全浏览器浏览器和SSL VPN 网关完成通信数据的完整性和机密性保护； 机房间通过IPSEC VPN保障通信数据的完整性和机密性。	符合	
9		网络边界访问控制信息的完整性	宜	SSL VPN网关对网络边界访问控制信息基于HMAC-SM3进行完整性保护。	（部分）符合	
10		安全接入认证	可	云平台接入侧部署SSL VPN网关，实现外网接入设 备的实体鉴别	符合	
11		密码服务	应	使用符合法律法规的相关要求并经商用密码认证机构认证合格的密码服务	符合	
12		密码产品	二级及以上	使用的密码产品达到 GB/T 37092 二级及以上安全要求	符合	

安全合规性表1

公共资源交易平台测试标专用
AE2C19CE67761GE1A62A8D6886A14DB9

设备和计算层技术符合度自评（三级）如下

No	分类	具体指标	要求	技术手段	符合情况	备注
13	设备和计算安全（15）	身份鉴别	应	云平台运维管理员和租户接入物理机和虚拟机进行管理前，需要通过安全网关进行身份鉴别。运维时，认证通过后接入堡垒机进行统一运维。	（部分）符合	集成USB-KEY、安全认证网关、SSL套件等满足
14		安全的信息传输通道	应	通过SSL VPN网关与浏览器间搭建的安全通信链路，完成对远程管理身份鉴别信息机密性的保护	（部分）符合	
15		系统资源访问控制信息完整性	应	云平台自身使用密码模块组件，基于AIDE等机制用SM3算法对设备资源访问控制信息、日志等进行完整性保护；（Host OS改造）		
16		重要信息资源安全标记完整性	宜	不涉及（云平台内未使用相关功能）		
17		日志记	宜	对云服务的操作日		

公共资源交易平台技术专用
AE2C19CE27646E

No	分类	具体指标	要求	技术手段	符合情况	备注
		录完整性		志基于SM3算法进行完整性保护；对系统运行日志、安全日志等复用OS通用机制保护		
18		重要可执行程序完整性	宜	云平台自身使用的通用服务器中重要程序和文件（包括虚拟机镜像模板等）在生成时利用数字签名进行完整性保护，使用或读取这些程序和文件时，进行验签以确认其完整性；私钥存放在物理密码机中，由物理密码机进行签名/验签操作；	部分符合	
19		密码服务	宜	使用符合法律法规的相关要求并经商用密码认证机构认证合格的密码服务	符合	
20		密码产品	应二级及以上	使用的密码产品达到 GB/T 37092 二级及以上安全要求 15-17等项软件产品实现国密功能支持	部分符合	

公共资源交易平台技标专用
AE2C19CEC77646E

No	分类	具体指标	要求	技术手段	符合情况	备注
				功		

安全合规性表2

应用和数据层技术符合度自评（三级）如下表：

No	分类	具体指标	要求	技术手段	符合情况	备注
21	应用和数据安全（30）	身份鉴别	应	1）云平台管理员和租户接入云平台管理平台和云服务应用前，需要通过IAM进行身份鉴别（对接CA支持商密证书的签发、验证，CA对接硬件加密机）。身份鉴别平台对云平台管理员/租户的身份鉴别方式为用户名/口令和智能密码钥匙/证书的双因素身份鉴别；	符合	集成USB-KEY、服务器密码机、商密SSL套件、KMS服务、CA等满足
22		访问控制信息完整性	应	云平台云管服务IAM等自身利用物理密码机或密码模块，采用HMAC-SM3对其访问控制策略进行完整性保护（改造中）；	（部分）符合	
23		重要信息资源	应	不涉及（云平台内未使用相关功能）	不涉及	

公共资源交易平台技标专用
AE2C19CEC77646E...

No	分类	具体指标	要求	技术手段	符合情况	备注
		安全标记完整性				
24		重要数据传输机密性	应	平台管理员/租户和云平台管理应用之间的数据传输：平台管理员/租户调用智能密码钥匙，云平台管理应用调用物理密码机或密码模块，采用SM2密钥协商算法进行会话密钥的交换，采用SM4算法和HMAC-SM3算法对传输数据进行机密性和完整性保护。	（部分）符合	
25		重要数据存储机密性	应	云平台云管等各服务内部的敏感数据、鉴别信息、租户信息等，调用KMS（对接物理密码机）或内置密码模块，采用SM4和HMAC-SM3算法对关键数据进行机密性和完整性保护，然后存放在数据库、磁盘中；	符合	

公共资源交易平台专用
AE2C19CE77646E1A6248D688EA14DB9

No	分类	具体指标	要求	技术手段	符合情况	备注
26		重要数据传输完整性	宜	同25项	（部分）符合	
27		重要数据存储完整性	宜	同26项	（部分）符合	
28		不可否认性	宜	不涉及（云平台内认为不涉及法律责任认定的应用）	不涉及	
29		密码服务	应	使用符合法律法规的相关要求并经商用密码认证机构认证合格的密码服务	符合	
30		密码产品	二级及以上	使用的密码产品达到GB/T 37092 二级及以上安全要求22-28等项软件产品实现功能为主，配套满足二级要求的HSM完成。	部分符合	

安全合规性表3

针对密钥管理，对称密钥管理技术符合度自评（三级）如下：

密钥分类	生成	分发	存储	使用	更新	导入导出	归档	撤销	备份恢复	销毁
物理密码机主	物理密码机内	不涉及该密钥	物理密码机内	物理密码机内	不涉及，由密码	不涉及该密钥	不涉及该密钥	不涉及	利用物理密码	物理密

公共资源交易平台技术标专用
AE2C19CEC776461A62185C88EA14DB9

密钥分类	生成	分发	存储	使用	更新	导入导出	归档	撤销	备份恢复	销毁
密钥（KMS 根密钥）	生成	分发	存储	部使用	机进行更新	的导入和导出	的归档		机自身的密钥备份和恢复机制实现	码机内部完成销毁
云平台管理主密钥	物理密码机内生成	不涉及该密钥分发	KMS 密钥管理系统数据库内存储	KMS 内部服务节点使用	定时更新	按需从 KMS 外部导入	不涉及该密钥的归档	不涉及	利用 KMS 的数据库备份机制实现	KMS 内部完成销毁
虚拟机迁移密钥	密码模块或物理密码机内生成	涉及该密钥分发，由 KMS 分发到指定服务和节点	平台管理主密钥加密存储	服务节点内部使用	定时或手动更新	一般不涉及该密钥的导入和导出	不涉及该密钥的归档	不涉及	利用服务节点自身的关键数据备份和恢复机制实现	服务节点内部完成销毁
云平台关键数据、访问控制信										

公共资源交易平台技术专用

密钥分类	生成	分发	存储	使用	更新	导入导出	归档	撤销	备份恢复	销毁
息、日志信息保护密钥										

安全合规性表4

非对称密钥管理技术符合度自评（三级）如下

密钥分类	生成	分发	存储	使用	更新	导入导出	归档	撤销	备份恢复	销毁
CA公钥	不涉及，由CA或PKI产生	以证书形式离线分发	以证书形式存储	以证书形式使用	不涉及，由CA进行更新	以证书形式离线导入和导出	不涉及该密钥的归档	不涉及，由CA进行撤销	不涉及，由CA进行备份恢复	不涉及，CA进行撤销操作
云平台管理应用私钥	签名私钥在物理密码机内生成，加	加密私钥由CA以离线方式进行分	物理密码机内存储	物理密码机内使用	支持更新	加密私钥以离线方式导入到物理	不涉及该密钥的归档	不涉及	利用物理密码机产品自身的密钥	物理密码机内销

公共资源交易平台技术专用
AE2C19CEC77646E1A62A8D88E14DB9

密钥分类	生成	分发	存储	使用	更新	导入导出	归档	撤销	备份恢复	销毁
	密私钥由CA生成	发，签名私钥不进行分发				密码机，签名私钥不进行导入导出			备份和恢复机制实现	毁
云平台管理应用公钥	签名公钥在物理密码机内生成，加密私钥由CA生成	以证书形式分发	以证书形式存储	以证书形式使用	定时或手动更新	以证书形式导入和导出	以证书形式归档	到期或按需撤销	以证书形式进行备份恢复	不涉及，由CA进行撤销操作
云平台管理员/租户私钥	签名私钥在智能密码钥匙内生成，	加密私钥由CA以离线方式进行分	智能密码钥匙内存储	智能密码钥匙内使用	支持更新	加密私钥以离线方式导入到智能	不涉及该密钥的归档	不涉及	不涉及该密钥的密钥备份和恢复	智能密码钥匙内

公共资源交易平台技术专用
ADBC19CEC77646E1A62A8BC88E1B3B9

密钥分类	生成	分发	存储	使用	更新	导入导出	归档	撤销	备份恢复	销毁
	加密私钥由CA生成	发，签名私钥不进行分发				密码钥匙，签名私钥不进行导入和导出				销毁
云平台管理员/租户公钥	签名公钥在智能密码钥匙内生成，加密私钥由CA生成	以证书形式分发	以证书形式存储	以证书形式使用	定时或手动更新	以证书形式导入和导出	以证书形式归档	到期或按需撤销	以证书形式进行备份恢复	不涉及，由CA进行撤销操作

安全合规性表5

3.2.4.4.1.8 密码安全管理制度

1. 密码算法及密码制度

本制度要求密码算法及密码技术必须符合相关法律法规要求，并结合信息系统密码应用基本要求进行密码应用安全建设。本制度中管理要求的密码算法和密码技术，主要公司业务使用的密码算法和密码技术。

公共资源交易平台技术专用
AD2C19CEC77646E1A62A8BC88E1DB9

2. 秘钥管理策略

密钥管理是整个云平台管理的核心问题，其主要是指密钥对的安全管理，内容包括云平台密钥管理与用户密钥管理。

密钥管理的主要目标是保证密钥在生成、备份、传递、使用、恢复、更新、销毁等整个生命周期中的安全。

1） 密钥生成

密钥采用人工产生或密码机产生密钥的方式，人工生成密钥成分时，将密钥分成不同的成分，每个密钥成分由不同的人员生成，采用数字和字母随机组合，并于密钥注入前规定时间内完成；密码机产生密钥时，由密码机生成导出。

密钥生成后，在硬件加密设备外部的明文形式由三段密钥组件构成。

2） 密钥传输

密钥在传输时采用双重控制和分裂学，分为三段组件，传输的方式采用多种传输渠道和不同传输时间的方法。

传输时存放密钥组件的介质为 IC 卡，每张 IC 卡只存放一段密钥组件。不存在传输完整密钥的情况。

3） 密钥注入

密码机主密钥、区域主密钥、成员机构主密钥，采用人工键入方式注入密钥组件的明文，且每段密钥组件由指定不同的密码操作员注入。

终端密钥注入，是由密码机生成密钥导出后，灌入母终端，再从母终端导入到其他终端。

工作密钥、终端 MAC 密钥是在终端进行签到时，已密文的方式进行传输，保存在终端里。

4） 密钥保管

对于密钥组件的存储，坚持三个原则：最小化、认可化和高安全性。

最小化：由密钥管理员负责保管密钥组件，且不同成分的密钥组件由不同人员保管；

认可化：密钥组件存放在封条封装的信封内，只有指定的密钥管理员可以拆分信封；

高安全性：封装密钥的信封存放在不同的保险箱内，密钥管理员才有保险箱

公共资源交易平台技标专用

的密码和钥匙。

对于密钥注入设备，密码操作员进行配置和维护。

5） 密钥泄漏与重置

除密钥泄漏或可能泄漏外，密码机主密钥（MK）一般不更新。成员主密钥（MMK）2—3 年更新一次或一般不跟新。若出现泄漏，则立即更换被怀疑或确认泄密的密钥，确定被涉及到的功能领域，并且向集客支撑中心报告。若主密钥和成员主密钥出现泄漏，采用与初次生成相同的控制方式产生新的主密钥和成员主密钥；若密码机主密钥（MK）泄漏，则替换主密钥并替换所有由该主密钥保护的密钥。若成员主密钥（MMK）泄漏，则替换成员主密钥并更换使用该成员主密钥加密的所有密钥。终端主密钥由密码机生成导出后，灌入母终端，再由母终端导入到其他终端里，如怀疑泄露，可通过母终端重新导入新密钥覆盖原先的密钥。工作密钥（WK）、终端 MAC 密钥采用联机签取的方式，每次签到都进行更新，若怀疑泄漏，则采用人工触发方式重置密钥。

6） 密钥删除与销毁

密钥生成后或在系统更新、密钥组件存储方式改变等情况时，不再使用的密钥组件（包括以纸质和 IC 卡方式存储的介质）或相关信息的资料均及时销毁。

作废或被损坏的密钥在双人控制下安全销毁，保证无法被恢复，销毁过程由专人监控和记录。

3. 密码建设管理

密码应用建设管理要求，主要是针对密钥安全需求、密码产品资质和功能项目签约、项目计划、项目实施和试运行相关阶段的安全管理要求。

在密码应用实施方面，对实施过程的控制方法和人员行为准则提出了要求。项目实施方首先应当制定详细的系统实施方案，并组织相关机构和专家对系统实施方案进行论证和审定。项目实施过程中，应保留相关文档和实施过程记录。

4. 设备管理

密码机共有两张管理员卡、三张密钥存储卡，每张磁卡都有口令保护。两张密码机管理员卡互为备份，用于密码机 root 用户的登录，以进行其他操作。密钥存储卡用于密钥的产生、备份、使用、恢复、更新、销毁等操作。在密码机的管理中，密码机管理员卡由密钥管理员保管，存放于集团核心区保险柜中。保险

公共资源交易平台投标专用

柜钥匙由集客支撑中心、集团客户部、网络与信息安全管理部保存，保险柜密码由文档管理员设定，保险柜内部存放管理员卡的抽屉钥匙有密钥管理员保存。密钥管理员卡的口令由密钥管理员设定。三张密钥存储卡，一张存于集客支撑中保险柜中，一张存于集团客户部保险柜，一张存于网络与信息安全管理部保险柜中。

当进行关于密钥的相关操作时，首先取出三张密钥存储卡和管理员卡，由密码安全审计员陪同，密钥管理员方可进行密钥的产生、备份、使用、恢复、更新、销毁等操作。

5. 秘钥信息安全

密钥信息包括密码机使用说明书、操作手册、密码机管理员卡、密钥存储卡和相关磁卡的口令密码信息等。其中密码机使用说明书、操作手册等资料属于核心资料，按照相关规定进行管理。密钥存储卡分由有集客支撑中心、集团客户部和网络与信息安全管理部保管，持卡人不得将管理员卡转借他人。所有卡的口令由密钥管理员设定，并制作密码信封归档备份。

6. 人员安全

密钥卡管理人员由可信员工担任，必须通过集团的背景调查，证实其可信性，并签署相关保密协议。

对密钥卡管理人员变动以及人员离职进行规范，相应权限(门禁)应及时变更，及时修改保险柜密码、交接钥匙和密钥卡，确保访问控制安全。

密钥卡管理人员不得将密钥卡随意放置，以免造成信息泄露。无关人员不得接触密钥卡。

密钥卡管理人员不得向任何第三方泄露密钥卡的相关信息。

非密码管理人员未经许可不得擅自上机操作和对运行设备及各种配置进行更改。

由于各种原因造成密钥信息泄露的相关人员要追究相应责任。

7. 密码产品日常管理

巡检记录：对机房密码产品运行状况的巡检所做的记录。

备份记录：对重要密码备份情况的记录。

密码安全事件记录：对涉及到密码安全的事件的记录。

密码产品运行事件记录：对密码产品一般性事件的记录。

公共资源交易平台投标专用

密码产品允许维护记录：包括密码产品的一般维护、安装调试、系统升级、故障处理。

密码产品变更记录：对密码产品发生变更的记录。

应具备各类完整的记录，格式可自行制定。各种记录至少保存一年，重要记录应长期保存。

8. 秘钥介质存储环境

1） 介质必须存放在指定场所，使用带密码锁的铁皮文件柜或保险柜存放介质。

2） 介质存储环境必须具有防潮、防盗、防火、防热、防尘、防磁以及防篡改、防泄露等保护措施。

3） 介质存储环境应指定专人负责管理，并每年至少进行一次检查和维护，确保存储环境的安全。存储环境应能够满足不断增长的

9. 密钥介质存档

1） 介质存档时，由介质交付单位填写介质存档审批表并签署意见后，由指定人员将介质交由介质管理员存入指定场所。

2） 介质交付前应密封牢实，密封处应有交付人的签字或盖章。重要介质交付前，介质中的数据应采取加密存储，并应对介质进行标识。

3） 介质存放指定场所后，介质管理员应对介质进行统一编号，并建立介质目录清单，清单内容至少应包括介质编号、介质交付单位、介质内容、介质类型、介质接收日期、介质交付人、介质接收人、介质重要程度、存放地点等信息。

4） 介质管理员应定期根据存档介质的目录清单对介质进行盘点。

5） 介质管理员应每年对介质进行一次检测、维护，确保介质的完整性、可用性。检测时可采用等距抽样或随机抽样方式进行。

6） 需要长期保存的介质，需与介质交付单位制定转存方案，根据转存方案和查询使用方法要在介质有效期内进行转存，防止存储介质过期失效。转存的介质必须有详细的文档记录。

10. 秘钥介质使用

1） 存储介质在计算机上使用前，应对使用环境进行技术检查，防止计算机因感染病毒或被植入恶意代码程序导致介质数据丢失、损毁。

公共资源交易平台投标专用

2） 介质使用人员应在规定时间内交还借用的介质，介质管理员应及时对交还的介质进行检查。

3） 介质不得接入或安装在非涉密计算机或低密级计算机上使用，不得转借他人，不得带离工作区，下班后应及时存放在指定场所。

4） 介质管理员应妥善保管存储介质，介质不使用时，应及时存放在指定场所。介质管理员岗位发生变化时，应及时和新任介质管理员进行介质管理交接手续。

11. 秘钥介质销毁

1） 未经批准任何人不得自行销毁存储介质。存储介质受损并且无法执行删除操作时，必须予以销毁。

2） 需要销毁存储介质时，必须填写存储介质销毁申请表， 报介质交付单位负责人批准同意后，方可实施。

3） 存储介质销毁时，应由介质管理员和介质交付单位人员在场确认，一人执行销毁一人负责监销，并做好介质销毁登记手续。

12. 秘钥管理要求

1） 采取加密技术等措施来有效保护密钥，以免密被非法修改和破坏。

2） 对生成、存储和归档保存密钥的设备采取物理保护。

3） 必须使用经过批准的密码机制进行密钥分发，并记录密钥的分发过程，以便审计跟踪。

4） 明确密钥的激活和去激活日期，即密钥生存期，使之只在生存期内有效，生存期的长短取决于使用环境及加密技术。

5） 密钥申请。需使用密钥者，应发起密钥申请流程，明确说明密钥使用范围、使用意图等。经审核人、审批人通过后，可获得密钥。

6） 密钥领用。密钥管理员根据用户的岗位及职责为其设置权限。用户签字确认密钥领用书后方可领取密钥。

7） 密钥使用。在密钥使用过程中，由于网络、系统或其他原因出现可疑指令，及时与维护人员联系。

8） 密钥变更。密钥持有人发生岗位变动时，将原密钥交给指定接收人，填制《个人保管使用办公物品交接表》，移交人、接收人、监交人签字完整后相关

公共资源交易平台投标专用

部门留档备查，接收人自行修改密码，密钥可继续使用。密钥管理员在密钥管理表上将该密钥的相关信息进行更新。

9） 密钥保管。密钥实行专人专管专用，不得擅自转借他人使用，密钥持有人离开岗位时，必须退出正在使用的系统，并将密钥从计算机拔出。重要密钥应放置于安全处，并实现双人控制，即独立保管不同权限的密钥。已作废密钥，交由资产管理放入安全处放置。同时密钥管理员在密钥管理表上将密钥的相关信息进行更新。

10）密钥备份与恢复。当系统出现故障导致密钥丢失，具备一定的备份恢复机制，确保系统可修复。密钥的备份应当进行严格的安全控制，包括从物理、安全技术、管理方面的严格控制。

11）应建立应对有关获取密钥的法律要求的程序，如需要作为法律证据时，加密信息可能需要采用解密形式提供。

12）要加强对公钥的保护，如采用值得信赖的，得到公认的认证中心来发布公钥证书，并且控制证书的发布和使用范围。

13）应在与外部加密服务提供商(如认证中心)之间的服务协议成合同中，涵盖责任、服务可靠性以及服务响应时同等内容。

14）在涉及使用加密技术、加密服务时，系统责任人必须正确评估并记录此类应用的风险。

3.2.4.4.1.9 密码管理岗位及职责

1） 组织形式

密码安全管理工作组由集团集客支撑中心领导任组长，由涉及密钥生命周期全过程的相关部门共同参加。

2） 工作职责

a） 按照规定，结合公司的实际状况，制定严格而有效的实施细则，落实岗位责任制；

b） 制订其他有关的安全专项管理制度，对涉及到密钥的生成、传输、保管各个环节的设备提出相应的安全管理要求，如出入登记制度、机房管理制度、岗位操作制度、密钥存储介质管理制度等。

c） 负责密钥生命周期，包括生成、分发与传输、注入与启用、保管、删除

公共资源交易平台投标专用

与销毁、泄漏与重置等各环节全方位、全过程的规范操作与安全管理。

d） 根据密钥特性，妥善保管密钥组件、密码函、IC 密码卡、软件、源代码、涉及密钥安全管理的各种文档。

e） 定期检查密钥安全管理状况，按规定填报有关表格、报告。

f） 网络与信息安全管理部可以定期或者不定期对信息机房管理工作中密码产品、使用和管理的情况进行检查和测评，对重要信息系统的密码配备、使用和管理情况每一年至少进行一次检查和测评。

遵循权限分离原则，设置密钥管理员、密码安全审计员、密码操作员等，且关键位置采用双人控制，即必须由两人验证通过后可访问或使用。

1） 系统用户增加和权限设置应由专人负责管理。

2） 系统维护人员需与业务操作人员相互分离。

3） 设备与系统的管理和使用补的多人共用。

4） 其他部门权限设置由直属领导提出申请，报分管领导审批后，由系统维护人员增设相关功能权限。

5）权限设定应遵循最小特权原则

NO	岗位	职责说明	岗位或人员匹配
1	密钥管理员	职责： 1)负责公司密钥管理中心的管理协调工作，负责制定密钥管理工作规划和应急措施及工作机制等制度规定； 2)负责信息系统中密钥的全生命周期管理，即产生、分发、存储、使用、更新、归档、撤销、备份、恢复销毁等环节的管理； 3)制止不正确操作，杜绝违规操作或者超越权限操作的行为； 4)严格考察本单位重要岗位的工作状况，对不适合密钥维护工作或者发现有不良行为的人员，提出调整要求；	

公共资源交易平台投标专用

		5)协助完成定期或者不定期的专项辅导检查工作； 6）同时履行密钥注入、保管等工作职责； 7）按照信息择分、随机性、不可测等原则生成密钥组件； 8）分别保管主密钥组件； 9）接受密钥资料（组件），验收接收到的新密钥资料是否受损； 10）协助完成定期或者不定期的专项辅导检查工作； 11）在监督下，完成密钥组件备份介质、文档等密钥资料的销毁。	
2	密码操作员	职责： 1）密码设备的主要操作，负责密码机等密码设备的界面操作，协助完成密钥生成、装载等操作过程； 2)维护密码机等密码设备保持良好的运行状态。	
3	密码安全审计员	职责：对密钥管理员和密码操作员的行为进行安全审计。	

密码权限管理表

3.2.4.4.1.10密码应急管理

云平台预案是在云平台基础上，针对密码泄露或破坏对业务产生的影响，准备和实施的应急处理方案，其基本价值在于：在突发密码安全事件出现之前就已经制定相应措施，做好一定准备；一旦安全事件发生，可以提供和实施这些替代方案，以最大限度地争取时间，减少损失。

根据网络与信息安全突发事件可控性、严重程度和影响范围的不同，分为以下四级：

公共资源交易平台投标专用

I 级（特别重大）：云发生性瘫痪，对正常工作造成特别严重损害，且事态发展超出控制能力的安全事件；

II 级（重大）：云发生大规模瘫痪，对正常工作造成严重损害，事态发展超出单一部门自身控制能力，需相关部门协同处置的安全事件；

III 级（较大）：某一区域的云瘫痪，对正常工作造成一定损害，但集客支撑中心可自行处理的安全事件；

IV 级（一般）：某一局部网络或者受到一定程度损坏，对某些工作有一定影响，但不危及整体工作的安全事件。

当相关部门发现计算机访问数据库速度迟缓、不能进入相应程序、不能保存数据、不能访问网络、应用程序非连续性工作时，要立即向集客支撑中心报告。集客支撑中心工作人员对各工作站提出的问题必须高度重视，做好记录，经核实后及时给各工作站反馈故障信息，同时召集有关人员及时进行讨论，如果故障原因明确，可以立刻恢复的，应尽快恢复工作；如故障原因不明、情况严重、不能在短期内排除的，应立即报告集团领导，在网络不能运转的情况下由集团领导协调相关部门工作，以保障云平台服务工作的正常运转。但是否启动应急预案需要参照以下描述执行：

机房主服务器发生不可抗拒因素（不可预知的突发故障）导致云服务停止运行 15 分钟以上时。

突发供电系统大范围停电，供电系统不能及时修复，并且备用电源亦不能提供电源，造成全部电脑不能运行。

遇地震、火灾、水灾等不可抗拒因素且对云服务造成大面积影响，导致云平台业务不能访问，或基础网络系统不能访问。

一旦发生上述情况之一，应迅速启动集团应急预案，但须遵守以下流程：支撑中心在第一时间汇报部门领导，如遇夜间或节假日有关使用部门立即上报总值班，总值班通知支撑中心人员，支撑中心人员到场后作出初步结论，汇报部门领导，由部门领导决定启动应急预案，并通知集团客户部及其他相关部门。集客支撑中心开展相应的处理，如发生不能自行处理的因素，立即通知签约的服务商、其他部门派人员到场处理。

1） IV 级故障由集客支撑中心完成应急响应工作；

2） III 级故障由信息安全领导小组牵头下，依靠自身信息技术人员、供应商完成应急响应；

3） I 级、II 级故障协调第三方服务机构、完成应急响应；

3.2.4.4.1.11密码人员管理

人员录用的应以相关管理规定为标准：对应聘者进行审查，确认其具有基本的专业技术水平，接受过安全意识教育和培训，能够掌握安全管理基本知识；对股份公司关键岗位的人员还应注重思想品质、历史方面的考察；

在签署劳动合同前，应由人力资源部进行人员背景、资质审查，技能考核等，合格者还要签署《保密协议》方可上岗；安全管理人员应具有基本的系统安全风险分析和评估能力；

关键区域或部位的安全管理人员应选用实践证明精干、内行、忠实、可靠的人员，必要时可按机要人员条件配备。

人员离岗的应以相关管理办法为标准：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限；收回所有相关证件、徽章、密钥、访问控制标记等；收回机构提供的设备等；

调离后的保密要求：管理层和股份公司关键岗位人员调离岗位，必须经人力资源部严格办理调离手续，承诺其调离后的保密要求；

离岗的审计要求：涉及组织机构管理层和股份公司关键岗位的人员调离单位，必须进行离岗安全审查，在审查合格后，方可调离；

对于在组织内进行岗位调动的员工，须根据新岗位的需要，增加、删除或修改该人员的计算机股份公司访问权限，包括电子邮件系统、业务应用系统、网络系统和其他计算机信息软硬件系统。与原岗位有关的所有资料文件，包括其软硬拷贝都需要移交，不允许私自带走。

定期的人员考核：每半年对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考；

定期的人员审查：对密码管理人员，包括密钥管理员、密码操作员、密码安全审计员，每半年进行审查，如发现其违反安全规定，控制使用；

全面严格的审查：对所有安全岗位人员的工作，通过全面考核进行审查，如发现其违反安全规定，应采取必要的应对措施。

公共资源交易平台投标专用

应知应会要求：应让股份公司相关员工知晓信息的敏感性和信息安全的重要性，认识其自身的责任和安全违例会受到纪律惩罚，以及应掌握的信息安全基本知识和技能等；

有计划培训：制定并实施安全教育和培训计划，根据不同培训对象的需要，每半年或每年进行一次安全培训，培养股份公司各类人员安全意识，并提供对密钥安全政策和操作规程的认知教育和训练等；

针对密码管理人员（包括密钥管理员、密码操作员、密码安全审计员），制定专业培训计划，包括密钥知识、密码安全技术、密码安全标准、密码安全要求、密码法律法规和业务控制措施等；

密码管理人员（包括密钥管理员、密码操作员、密码安全审计员）按照培训计划完成培训后需通过考试方可上岗。

按人员资质要求培训：对所有工作人员的安全资质进行定期检查和评估，使相应的安全教育成为组织机构工作计划的一部分；

培养安全意识自觉性：对所有工作人员进行相应的安全资质管理，并使安全意识成为所有工作人员的自觉存在。

对硬件和软件维护人员，咨询人员，临时性的短期职位人员，以及辅助人员和外部服务人员等第三方人员签署包括不同安全责任的合同书或保密协议；规定各类人员的活动范围，进入计算机房需要得到批准，并有专人负责；第三方人员必须进行逻辑访问时，应划定范围并经过负责人批准，必要时应有人监督或陪同；

在重要区域，第三方人员必须进入或进行逻辑访问（包括近程访问和远程访问等）均应有书面申请、批准和过程记录，并有专人全程监督或陪同；进行逻辑访问应使用专门设置的临时用户，并进行审计；

关键区域管理要求：在关键区域，不允许第三方人员进入或进行逻辑访问；如确有必要，除有书面申请外，可采取由机构内部人员带为操作的方式，对结果进行必要的过滤后再提供第三方人员，并进行审计；必要时对上述过程进行风险评估和记录备案，并对相应风险采取必要的安全补救措施。

违反本管理制度，将视情节提请给与相应的责任人批评教育、通报批评、行政处分或处以警告，以追究其责任。触犯国家法律、行政法规的，依照有关法律、行政法规的规定予以处罚；构成犯罪的，依法追究刑事责任

公共资源交易平台技标专用

为加强对保密工作的组织和领导和管理，防止各类重要信息失密、泄密、窃密，设立保密工作领导小组，负责对保密工作的管理与考核。

相关部门设立保密员，每季度由负责人组织相关部门保密员召开保密会议，保密员负责对本部门保密工作的日常管理。

所有工作人员需签订书面的《保密协议》，并作为劳动合同附件。且在岗职员必须严格执行《保密协议》规定。

第三方工作人员须签订《第三方人员安全保密协议》，同时必须严格按照规定执行，若违规者将根据合同进行处置。

3.2.4.4.2 租户密码应用安全方案

3.2.4.4.2.1 方案概述

本项目需要提供一套租户业务密码测评服务。提供业务密码服务能力，包括加解密服务、校验服务、签名验签服务、时间戳服务、秘钥管理服务、数据库加密服务、SSL 安全网关、国密浏览器、USBKEY 等。**本项目需要提供 1 套租户密评套件。**

序号	服务分类	规格	服务说明	单位	数量
44	密码应用安全服务	加解密服务	独享虚拟密码机进行数据加解密服务，SM4 对称加解密能力 250Mtps，最大并发 500M。	套	1
45		完整性校验服务	独享虚拟密码机进行数据完整性校验服务，SM3 完整性校验能力 62Mtps，SM4 完整性校验能力 250Mtps，最大并发 500M。	套	1
46		签名验签服务	SM2、SM3 签名验签能力 250Mtps，最大并发 500M。	套	1
47		时间戳服务	提供可靠的时间服务，具体包括业务系统对接、密码系	套	1

公共资源交易平台技术专用
AE2C19CEC77546C162A8BC88EA4DB0

			统对接、密码模块对接。并发连接数：300，守时精度：<0.5ms（72 小时），产生时间戳速度 300 次/秒，时间戳签发：200 次/秒，时间戳验证：120 次/秒；		
48		密钥管理服务	依托密码基础设施提供密钥管理服务，提供密钥的全生命周期集中管理。服务并发速率≥300，密钥对生成速率≥300 对/秒，可管理密钥对容量≥300 对。	套	1
49		数据库加密服务	提供数据库机密性和完整性保障。存量（300W）数据加/解密：1.5 万条/秒，加密表插入速率:6000 条/秒，加密表查询速率：4000 条/秒。	套	1
50		SSL 安全网关	国密 VPN 安全网关，提供业务用户安全接入，包括通信双方身份鉴别、网络通道加密。	套	1
51		国密浏览器	提供支持国产商用密码算法的安全浏览器，包括 SM2/SM3/SM4 国密算法以及国密的 SSL 协议。	套	1
52		USBKey	提供终端密码模块运算、密钥安全管理能力。SM4 加/解密速率≥1 Mbps，SM2 加/	套	2

公共资源交易平台投标专用
AE2C19CEC7764E1A6248BC88EA14DB9

			解密速率≥0.6Mbps,SM2 签名速率≥50.96 次/秒，SM2 验签速率为 70 次/秒，SM3 运算速率≥1Mbps。		

密码是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。《中华人民共和国密码法》的颁布实施，从法律层面为开展商用密码应用提供了根本遵循依据，《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。为贯彻落实《中华人民共和国密码法》关于信息系统密码应用的要求，结合《国家电子政务建设指导意见》，决定对已经建成的云上业务系统进行密码应用改造。

通过对系统的现状和密码应用需求进行分析，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等4个层面，以及密钥管理、安全管理等方面，设计了该系统密码应用的技术方案、安全管理方案和实施保障方案。

本项目为上业务系统提供通过密评所需的密码服务，包括证书服务、密钥管理服务、加解密服务、身份认证服务、签名验签服务、签章服务、时间戳服务、协同签名服务等。围绕GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中关于信息系统在系统规划阶段的密码应用要求，综合考虑物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的密码应用方案，满足GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标要求，确保信息系统可正常通过密码应用安全性评估。

本方案设计，遵循以下原则：

1） 总体性原则

通过从整体层面，对本系统的密码应用开展顶层设计，明确密码应用需求和预期目标，并与本系统网络安全保护等级相结合，通过系统的设计形成涵盖技术、管理、实施保障的整体方案，为在本系统中落实密码应用相关要求奠定基础。

2)　完备性原则

围绕本系统实际业务应用与安全保护等级，站在整体角度，通过自上而下的体系化设计，综合考虑物理和环境安全、 网络和通信安全、设备和计算安全、应用和数据安全等多个层面密码应用需求，设计本系统密码改造方案。

3)　经济性原则

结合系统规模，在合理、够用的前提下，设计满足GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的密码应用改造方案，确保本系统密码应用改造投资合理，规模适度，避免资金浪费和过度保护。

4)　自主可控，安全合规

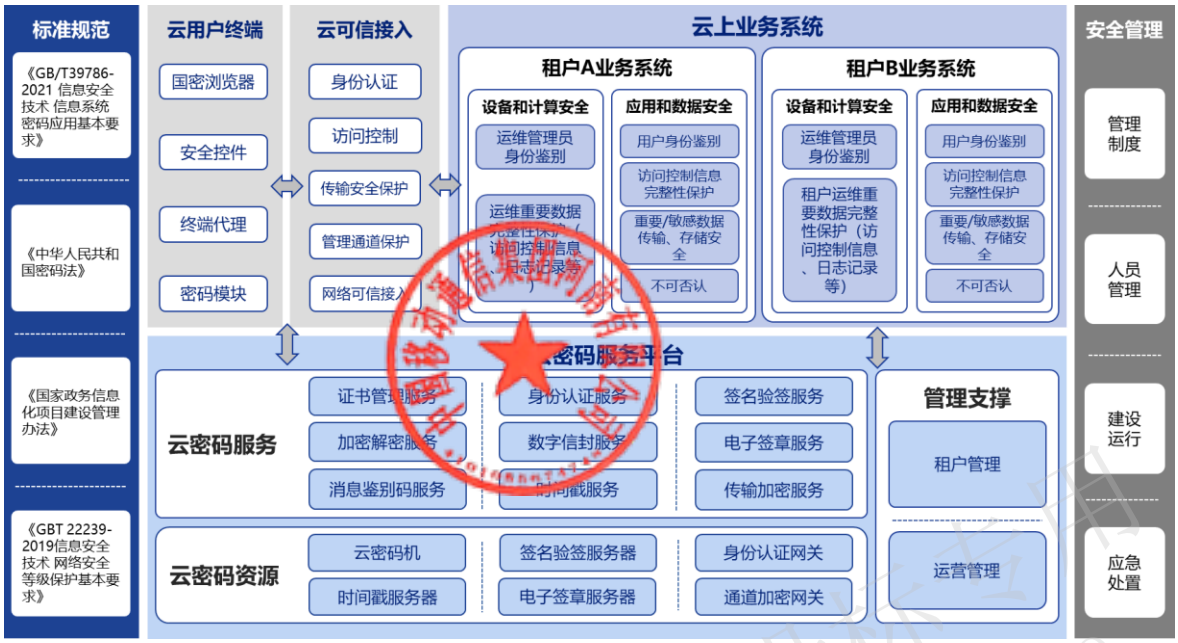
为云上业务系统提供密码服务的底层密码产品基于国产自主可控软硬件平台开发，实现系统的安全可信，采用具有商用密码认证的设备、产品，实现密码算法使用的正确性和密码应用的合规性。

5)　总体规划、分步实施

根据《信息安全技术 信息系统密码应用基本要求》，从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据等四个安全层面，按照“总体规划、分步实施”的原则开展信息系统密码应用建设工作。在规划、设计阶段，对信息系统在各个层面涉及的安全问题进行全面分析，并制定详细的密码应用方案。在建设阶段，结合项目建设周期、预算等实际情况，在保证信息系统满足安全性、合规性、可用性等前提下，制定密码应用分步实施计划，通过分阶段实施，逐步提升信息系统密码应用水平。

公共资源交易平台技术专用

3.2.4.4.2.2 平台架构设计



根据云上业务系统密码应用需求设计相应的密码应用技术框架，在设计时遵循总体性、完备性、经济性、高可靠、可扩展等原则，同时遵循《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》、《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》等相关标准规范。技术框架从下到上依次分为云密码服务平台和云上业务系统密码应用两部分。

云密码服务平台由云密码资源和云密码服务两部分组成，云密码资源和服务共同构建云密码资源池，为云上业务系统提供密码支撑服务，其中云密码资源提供基础的密码算法，云密码服务是通过调用云密码资源中的各种基础密码服务，为云上业务系统提供统一的密码服务，包含证书管理服务、身份认证服务、签名验签服务、消息鉴别码服务、加密解密服务、数字信封服务、电子签章服务、时间戳服务等，满足云上业务系统对于密码服务的不同需求。

云密码应用包括云用户终端密码应用、云可信接入密码应用和云上业务系统密码应用三部分。

1、 云用户终端密码应用为云用户终端提供密码安全服务，包括国密浏览器、安全控件、终端代理和密码模块。云用户终端使用终端密码服务发起身份认证，安全加密通道建立等，保障云用户终端本身安全以及云用户终端和云上业务系统的网络通信安全。

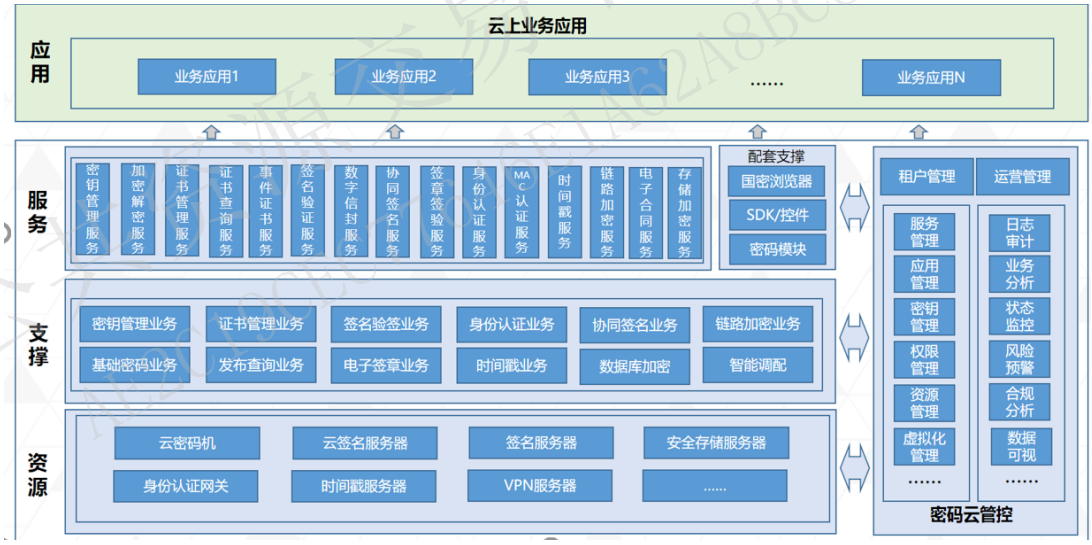
2、 云可信接入密码应用为云上业务系统可信接入提供安全密码服务，保障接入云上业务系统的终端安全可信以及网络通信安全等，包括身份认证、访问控制、传输安全、管理通道加密和网络可信接入。

3、 云上业务系统密码应用使用云密码服务平台提供的各种密码服务满足云上业务系统的密码安全需求。

3.2.4.4.2.3 云密码服务平台部署架构

密码服务资源池部署在政务云中，每个REGION部署一套

云密码服务平台，是整个密码安全基础设施的管理运营保障，统一管理总体技术架构中的云密码资源、云密码服务，云密码服务平台包括服务、支撑、资源和密码云管控四部分，为云租户提供数据加解密服务、密钥管理服务、签名验签服务、身份认证服务、签章服务、数字证书服务等各类密码服务，通过云密码机、云签名验签服务器、身份认证网关等各类密码资源，进行有效的服务支撑，满足云租户的各类密码使用场景需求，实现安全、合规、完整的密码安全治理。



服务层：服务层包括密钥管理服务、加密解密服务等各类密码服务，这些服务提供密码相关的服务集合为云上业务应用进行服务支撑，并提供国密浏览器、SDK/控件、密码模块等配套支撑解决相关问题。

支撑层：支撑层包括密钥管理业务、基础密码业务等，可以有效解决云上业务系统商用密码使用的合规性、正确性和有效性的问题，这些支撑层的系统是密码服务平台的核心，处理着从服务层进来的云上业务应用系统密码服务请求

和密码业务实现。

资源层：资源层包含云密码机、云签名验签服务器等各类密码设备，共同组成了云租户密码资源池，支持硬件密码设备的基本配置管理和实现各类密码设备资源的合理分配和共享使用，同时还支持按设备类型划分设备组管理，以保障密码设备资源可以更高效和可靠的为云上业务应用提供密码安全服务。

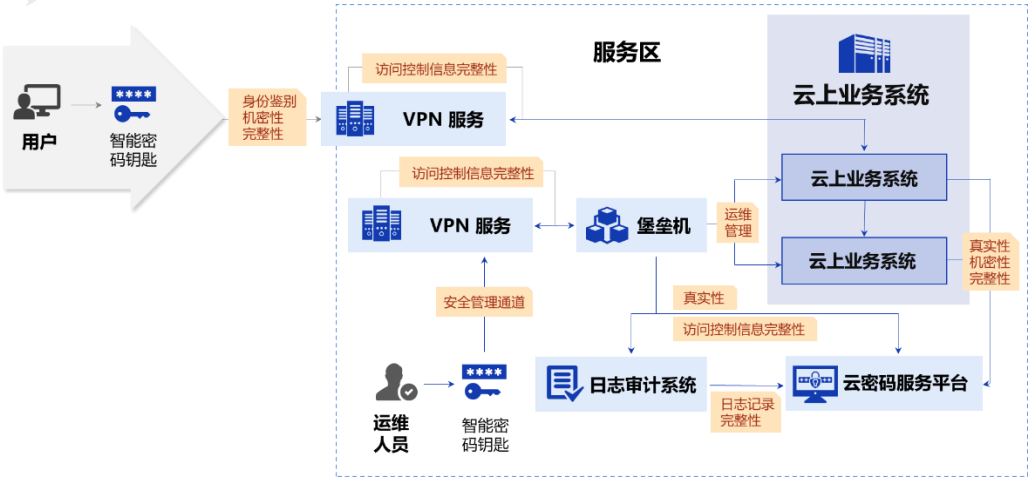
密码云管控：包括服务管理、应用管理等各类服务，将各类密码服务能力变成云上的一种资源服务赋能所有客户、软件和互联网应用，同时日志审计、业务分析、状态监控等功能共同形成了运营管理能力，为云租户提供有效的运营保障，租户管理与运营管理共同组成了密码云管控体系。

密码服务平台支持租户管理模式，即一套密码服务平台可为多个委办局的业务系统提供独立的密码服务，每个委办局作为一个独立的租户，可以进行租户内的应用管理、密钥管理、密码应用的统计分析等功能，租户之间密码资源彼此隔离，确保各自密钥的管理和使用安全。

密码服务平台为多个租户的业务系统提供密码服务，可根据各个租户的业务需求提供不同规格的密码服务能力，支持按数量、时长等方式进行计费、续费和扩容管理等，支持整体平台服务、镜像、资源等各维度的监控预警，应用、服务、设备等维度的统计分析，以及支持平台密码业务管理和密码服务运营的综合数据展示能力。

3.2.4.4.2.4 详细设计

3.2.4.4.2.4.1 概述

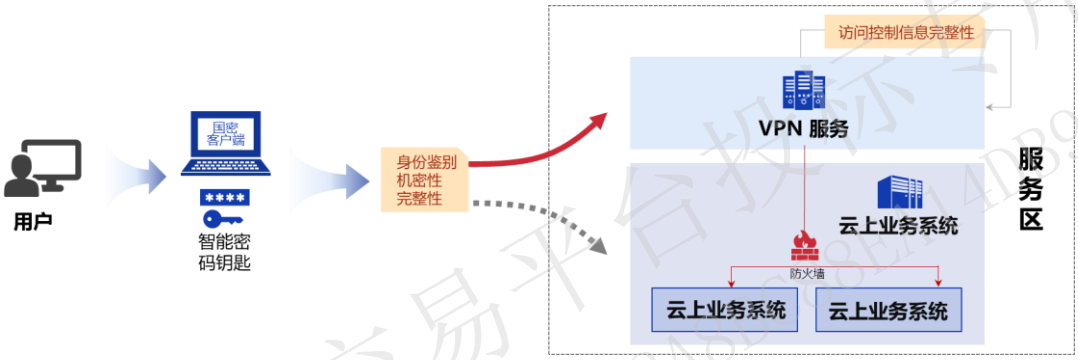


云上业务系统部署在云平台上，为终端用户提供各种业务服务。针对云上业务系统，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等不同技术层面进行方案设计，保证云上业务系统密码应用的合规性、正确性和有效性。

3.2.4.4.2.4.2 物理和环境安全

由于云上业务系统部署在政务云平台，使用了云平台提供的虚拟设备资源，因此物理和环境安全部分依赖于云平台所在的物理机房。

3.2.4.4.2.4.3 网络和通信安全



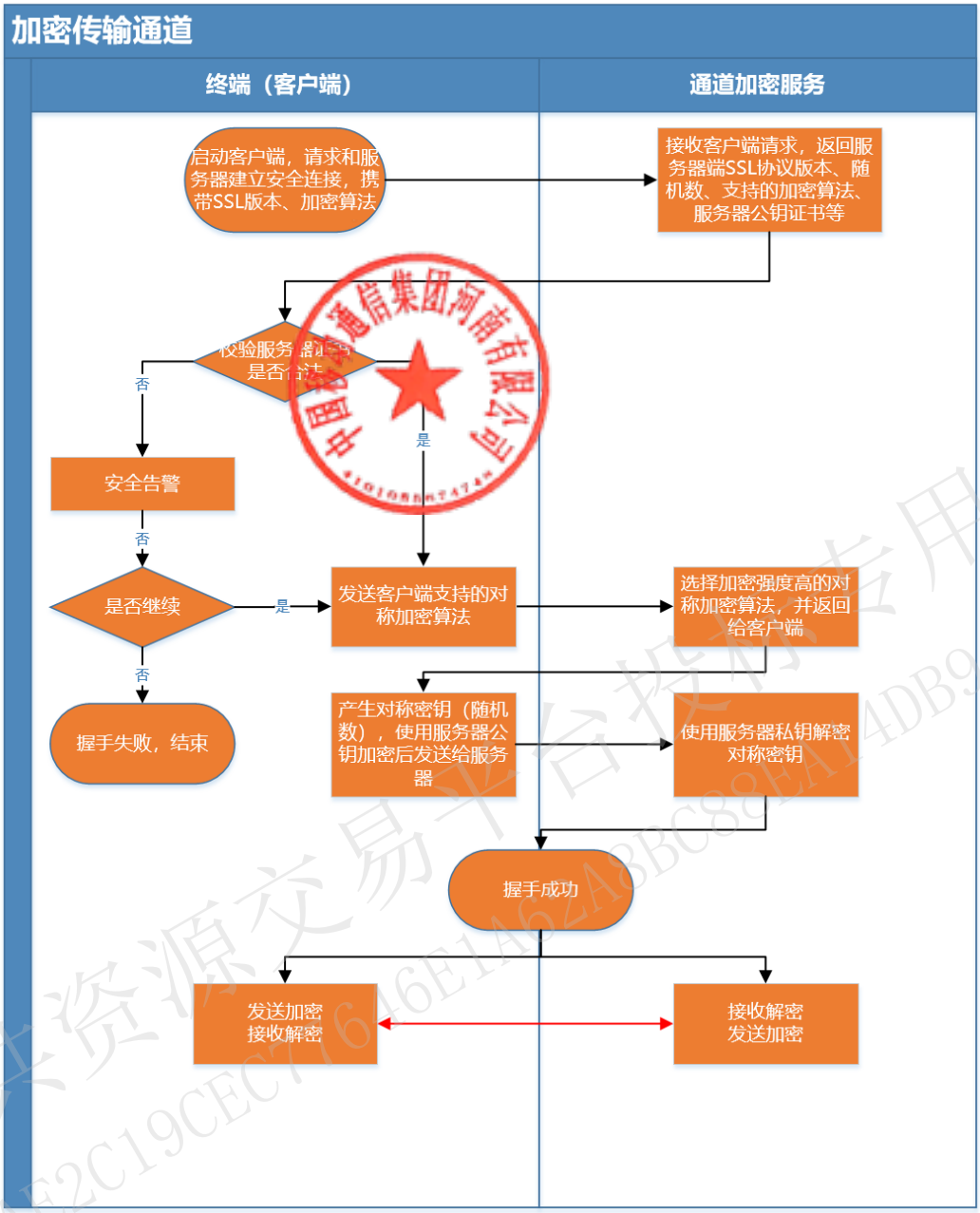
给终端用户配备智能密码钥匙或安装软件密码模块并内置用户数字证书，当用户访问云上业务系统时，需要出示身份信息，VPN安全网关对终端用户身份进行真实性验证，验证通过可正常访问云上业务系统。

网络边界访问控制信息存储在VPN安全网关，VPN安全网关内部使用HMAC-SM3等密码技术保障访问控制信息的完整性。

在“应用和数据安全”层面，针对云上业务系统涉及的重要数据采用符合要求的密码技术进行保护，保证重要数据传输的机密性。

通过通道加密服务和防火墙策略配合，构建用户访问云上业务系统的安全访问通道。终端用户使用智能密码钥匙或软件密码模块，通过国密客户端和通道加密服务构建加密传输通道，实现通讯过程中数据传输的完整性保护。

公共资源交易平台投标专用



1）客户端向服务器传送客户端SSL协议的版本号，加密算法的种类，产生的随机数，以及其它服务器和客户端之间通讯所需要的各种信息；

2）服务器向客户端传送SSL协议的版本号，加密算法的种类，随机数以及其他相关信息，同时服务器还将向客户端传送自己的证书；

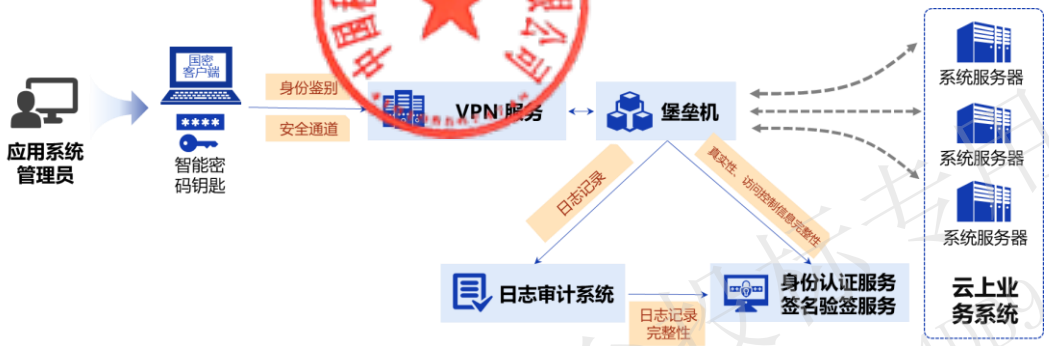
3）客户端利用服务器传过来的信息验证服务器证书的合法性，服务器的合法性包括：证书是否过期，发行服务器证书的CA是否可靠、服务器证书上的域名是否和服务器的实际域名相匹配；

4）客户端随机产生对称密钥，使用服务器证书公钥对产生的对称密钥进行加密，然后将加密后的信息传给服务器；

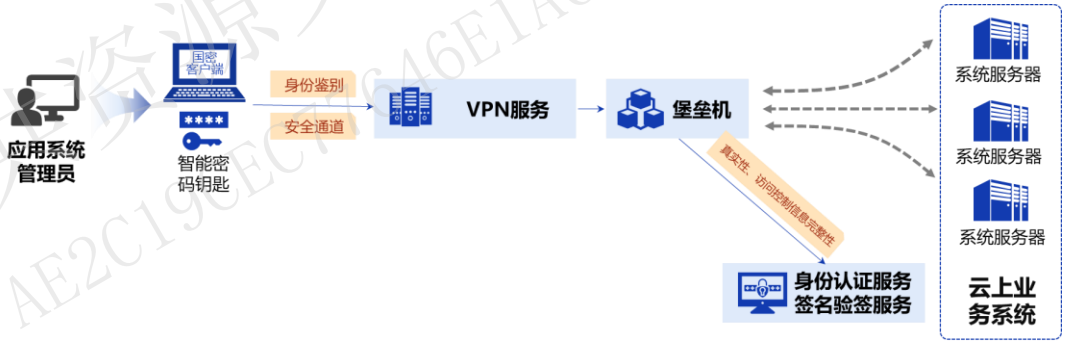
5）服务器用自己的私钥解密对称密钥；

6）客户端和服务器端使用相同的对称密钥对传输数据进行加密，加密传输通道建立完成。

3.2.4.4.2.4.4 **设备和计算安全**



在管理通道上部署堡垒机，通过堡垒机对服务器进行集中运维管理。同时在管理通道上部署VPN安全网关，管理员使用智能密码钥匙首先经过VPN安全网关的认证，完成管理员身份鉴别。

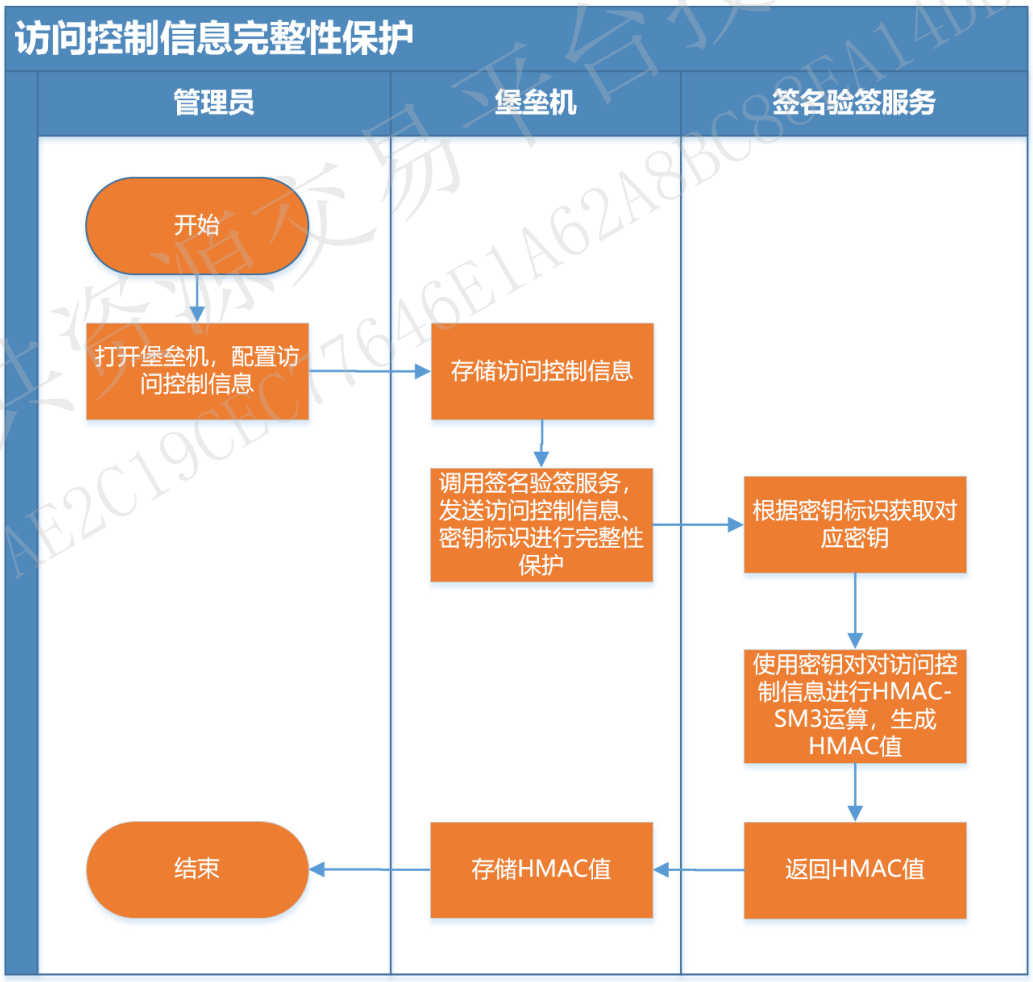


在管理通道上部署堡垒机设备，通过堡垒机对服务器进行集中运维管理。同时在管理通道上使用通道加密服务，管理员使用智能密码钥匙，通过国密客户端和通道加密服务构建加密传输通道，实现远程管理通道安全。



通过堡垒机对云上业务系统服务器设备进行集中运维管理，堡垒机里维护了针对运维管理的核心访问控制信息，需要对这些访问控制信息进行安全防护。堡垒机通过调用签名验签服务采用HMAC-SM3密码技术对堡垒机内的访问控制信息进行完整性保护。当访问控制信息进行变更时，需要重新调用签名验签服务对访问控制信息进行完整性保护。当管理员登录堡垒机时，堡垒机通过调用签名验签服务对访问控制信息进行完整性验证。

访问控制信息完整性保护流程如下：



1） 管理员访问堡垒机，配置访问控制策略；

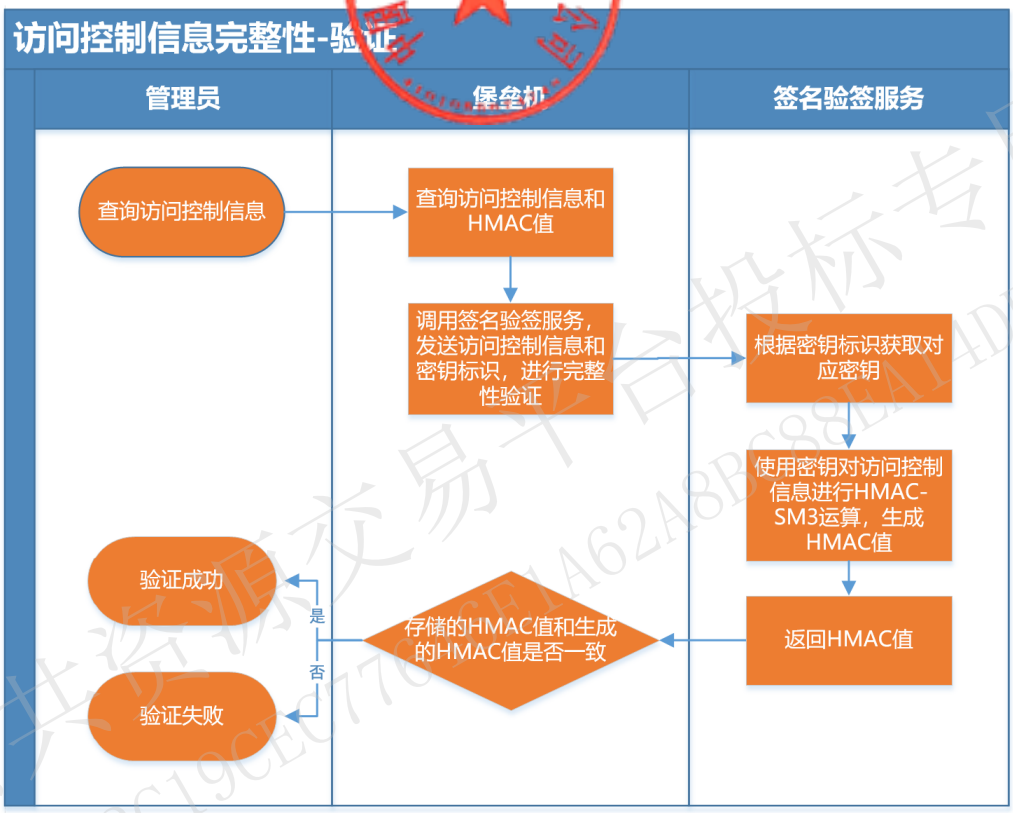
公共资源交易平台投标专用

2） 堡垒机保存访问控制策略，同时调用签名验签服务，发送访问控制信息、密钥标识进行完整性保护；

3） 签名验签服务根据密钥标识查询对应密钥，并对访问控制信息进行HMAC-SM3运算，生成HMAC值；

4） 签名验签服务将HMAC值返回给堡垒机；

5） 堡垒机存储HMAC值。



1） 管理员登录堡垒机，查询访问控制信息；

2） 堡垒机调用签名验签服务，发送访问控制信息、密钥标识，进行完整性验证；

3） 签名验签服务根据密钥标识获取对应密钥，并使用密钥对访问控制信息进行HMAC-SM3运算，生成HMAC值；

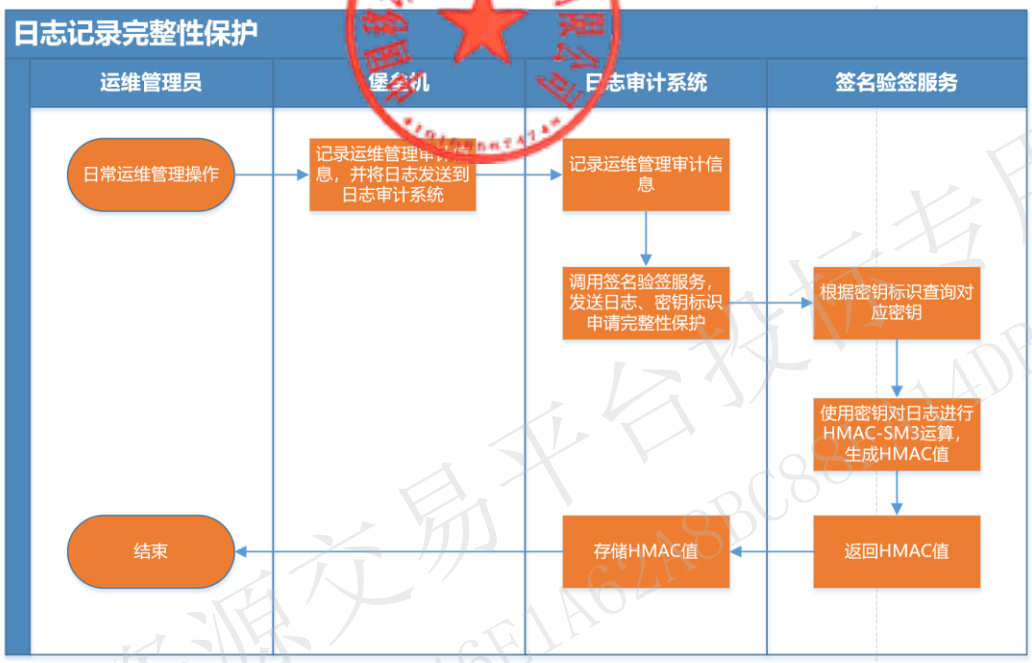
4） 签名验签服务将HMAC值返回给堡垒机；

5） 堡垒机比较HMAC是否一致，如果一致，表示访问控制信息完整性未被破坏，如果不一致，表示访问控制信息完整性被破坏。

公共资源交易平台投标专用

云上业务系统通过调用签名验签服务，针对重要信息资源安全标记进行完整性保护。

堡垒机将运维管理日志记录发送到统一的日志审计系统，日志审计系统通过调用签名验签服务，采用HMAC-SM3密码技术对对接收到的日志记录进行完整性保护，将日志记录和完整性信息存储到日志审计系统。在查询日志时，对日志记录进行完整性验证，防止日志信息被非法篡改。



1） 堡垒机记录运维管理员日常运维审计日志；

2） 堡垒机将日志发送到日志审计系统；

3） 日志审计系统调用签名验签服务，发送运维审计日志、密钥标识申请完整性保护；

4） 签名验签服务根据密钥标识获取密钥，并使用密钥对日志进行HMAC-SM3运算，生成HMAC值；

5） 签名验签服务将HMAC的值，返回给日志审计系统；

6） 日志审计系统存储HMAC值。

公共资源交易平台技术专用



1）管理员访问日志审计系统，查询日志信息；

2）日志审计系统调用签名验签服务，发送日志信息密钥标识申请完整性验证；

3）签名验签服务根据密钥标识获取密钥，并使用密钥对日志进行HMAC-SM3运算，生成HMAC值；

4）签名验签服务将HMAC的值，返回给日志审计系统；

5）日志审计系统比较HMAC是否一致，如果一致，表示日志信息完整性未被破坏，如果不一致，表示日志信息完整性被破坏。

3.2.4.4.2.4.5 应用和数据安全

身份鉴别

公共资源交易平台投标专用
ABC19CEC7646E1A62A8BC88EA14DB9

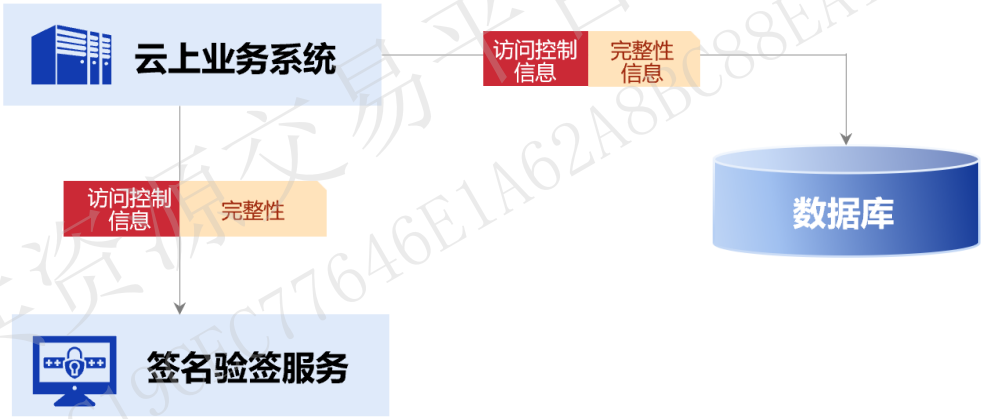


用户访问云上业务系统时，使用智能密码钥匙或软件密码模块中的数字证书发起身份认证，云上业务系统服务器通过调用身份认证服务对登录用户进行身份鉴别，保证用户身份的真实性。详细流程如下：

1）用户使用智能密码钥匙或软件密码模块中的数字证书发起身份认证；

2）云上业务系统服务器调用身份认证服务对用户进行身份鉴别，同时对用户证书进行有效性、状态等校验，验证通过则登录成功，否则登录失败。

访问控制信息完整性



云上业务系统通过调用签名验签服务，针对访问控制信息进行完整性保护。云上业务系统将访问控制信息和完整性信息存储到数据库，使用时对访问控制信息进行完整性验证，保证用户合法访问。



公共资源交易平台投标专用

重要数据传输机密性

客户端通过调用智能密码钥匙或软件密码模块的加密服务，对客户端向服务器传输的重要数据进行加密，云上业务系统服务器通过调用加解密服务，对向客户端传输的重要数据进行加密，保证双向传输过程中重要数据的机密性。详细流程如下：

终端用户向云平台提交数据时，通过调用智能密码钥匙或软件密码模块的加密服务，对客户端向云上业务系统服务器传输的重要数据进行加密，云上业务系统服务器通过调用加解密服务对数据进行解密，得到数据原文，保证客户端提交到云上业务系统服务器的重要数据的机密性。同时，云上业务系统服务器通过调用加解密服务，对向客户端传输的重要数据进行加密，客户端通过调用智能密码钥匙或软件密码模块对数据进行解密，得到数据原文，保证云上业务系统服务器发送给客户端的重要数据的机密性。详细流程如下：

1）客户端使用智能密码钥匙或软件密码模块中的密钥和加密服务对重要数据进行加密；

2）加密数据以数字信封方式传输给云上业务系统服务端，保障重要数据从客户端向服务器传输过程中的机密性；

3）云上业务系统服务器通过解密数字信封得到原文；

4）云上业务系统服务器调用加解密服务对重要数据进行加密，加密信息以数字信封方式传输给客户端，客户端解密数字信封得到原文，保障重要数据从云上业务系统服务器向客户端传输过程中的机密性。

重要数据传输完整性

客户端通过调用智能密码钥匙或软件密码模块的签名验签服务，对客户端向服务器传输的重要数据进行完整性保护，云上业务系统服务器通过调用签名验签服务，对向客户端传输的重要数据进行完整性保护，保证双向传输过程中重要数据的完整性。详细流程如下：

客户端通过调用智能密码钥匙或软件密码模块的签名验签服务，对客户端向云上业务系统服务器传输的重要数据进行完整性保护，云上业务系统服务器通过调用签名验签服务对数据进行完整性验证，保证客户端提交到云上业务系统服务器的重要数据的完整性。同时，云上业务系统服务器通过调用签名验签服务，对

公共资源交易平台投标专用

向客户端传输的重要数据进行完整性保护，客户端通过调用智能密码钥匙或软件密码模块对数据进行完整性验证，保证云上业务系统服务器发送给客户端的重要数据的完整性。详细流程如下：

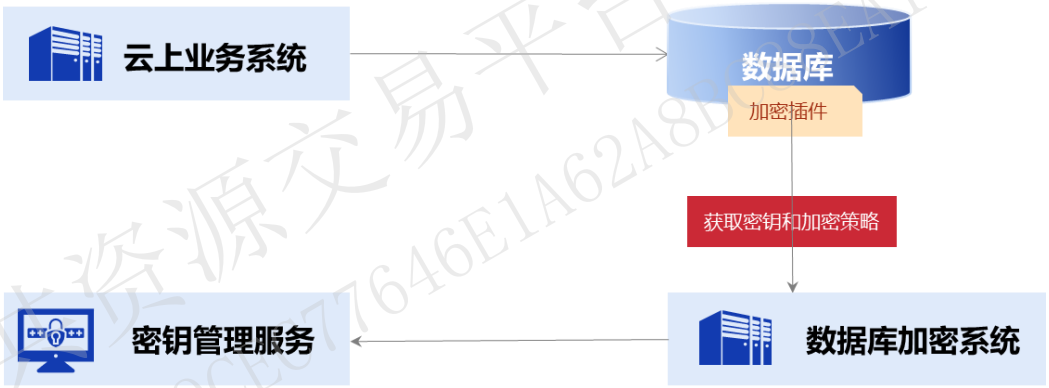
1）客户端使用智能密码钥匙或软件密码模块中的密钥和签名验签服务对重要数据进行完整性保护；

2）将重要数据以及完整性信息传输给云上业务系统服务器，保障重要数据从客户端向服务器传输过程中的完整性；

3）云上业务系统服务器调用签名验签服务对完整性信息进行验证；

4）云上业务系统服务器调用签名验签服务对重要数据进行完整性保护，将重要信息及完整性信息传输给客户端，客户端使用智能密码钥匙或软件密码模块中的签名验签服务对完整性信息进行验证，保障重要数据从云上业务系统服务器向客户端传输过程中的完整性。

重要数据存储机密性-透明加解密



部署数据库加密系统，同时在云上业务系统数据库服务器上部署数据库加密插件。云上业务系统进行数据存储时，加密插件连接数据库加密系统，获取加密密钥和加密策略，根据加密策略，使用加密密钥自动对重要数据进行加密，从而完成重要数据的机密性保护。详细流程如下：

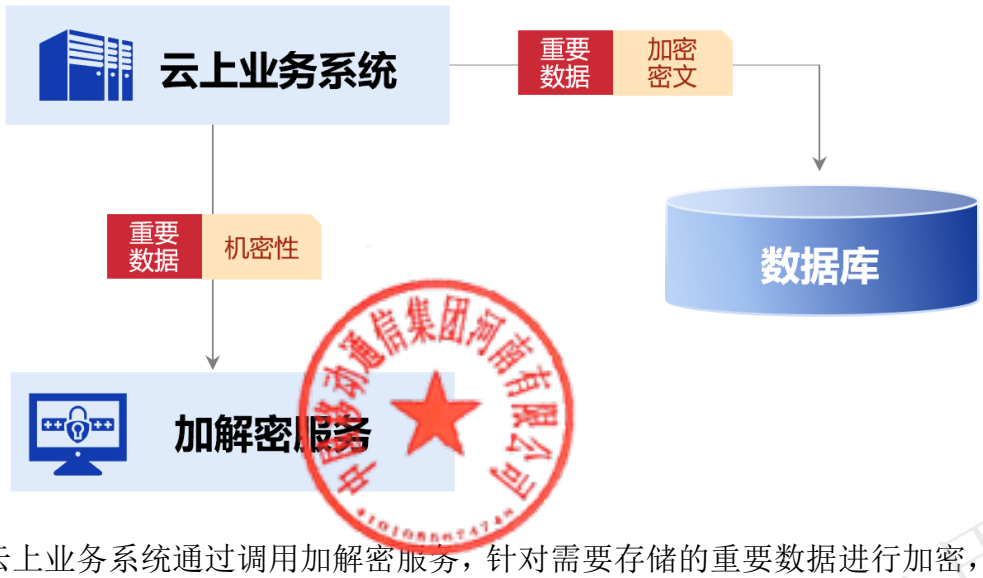
1）由密码服务平台为云上业务系统生成专属密钥；

2）云上业务系统要进行数据存储时，加密插件根据加密策略自动对数据进行加密存储，整个加密过程对管理员来说是透明的；

3）云上业务系统进行数据读取时，读取数据库中的存储内容加密插件自动对加密内容进行解密。

重要数据存储机密性-应用数据改造

公共资源交易平台投标专用



云上业务系统通过调用加解密服务，针对需要存储的重要数据进行加密，保证存储过程中关键信息的机密性。详细流程如下：

1）由密码服务平台为云上业务系统生成专属密钥；

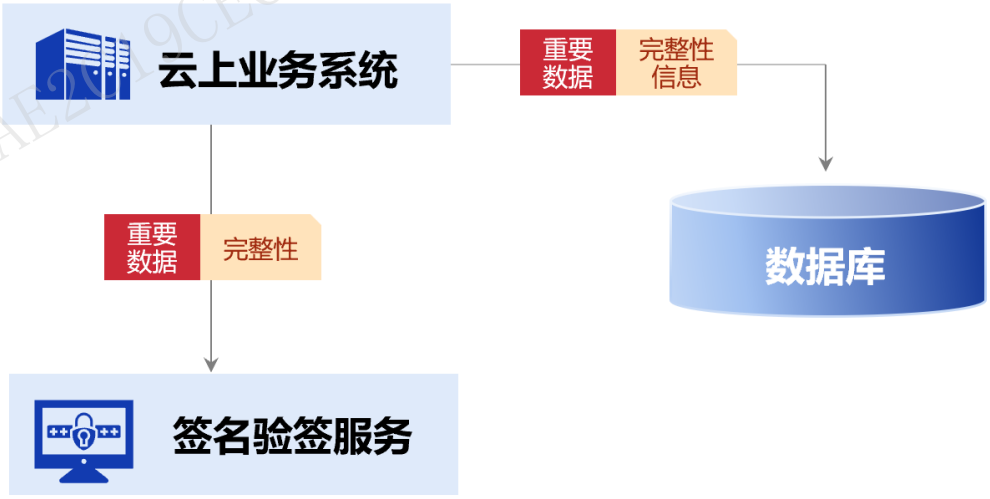
2）云上业务系统要进行数据写入存储时，调用密码服务平台产生密钥；

3）密码服务平台使用 SM4 算法对存储的重要数据进行对称加密；

4）密码服务平台将加密后的密文返回给云上业务系统，云上业务系统将密文存储在数据库中；

云上业务系统要进行数据读取时，读取数据库中的存储内容并调用加解密服务使用 SM4 算法对密文进行解密，得到存储数据的原文。

重要数据存储完整性



云上业务系统通过调用签名验签，针对需要存储的重要数据进行完整性保护，保证存储过程中重要数据的完整性。详细流程如下：

公共资源交易平台投标专用

1）由密码服务平台为云上业务系统生成专属密钥；

2）云上业务系统要进行数据写入存储时，调用签名验签服务使用 HMAC-SM3 算法对存储的重要数据生成完整性信息；

3）密码服务平台将完整性信息返回给云上业务系统，云上业务系统将完整性信息存储在数据库中；

4）云上业务系统要进行数据读取时，调用签名验签服务使用 HMAC-SM3 算法对数据进行完整性验证。

不可否认性

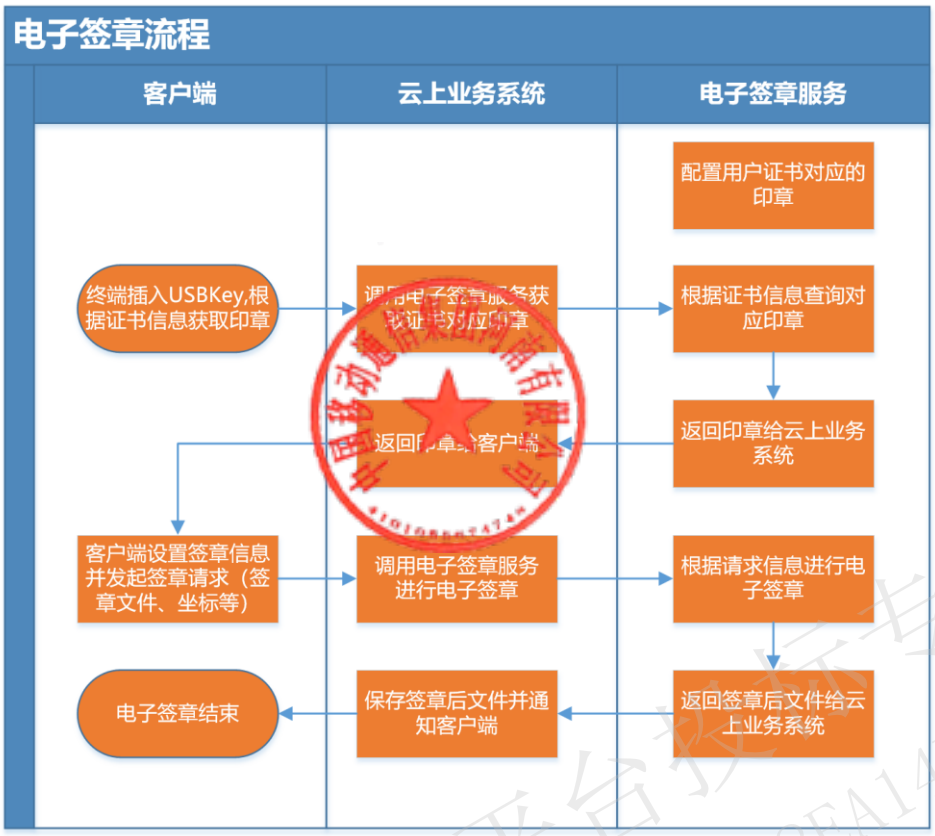
根据云上业务系统的密码使用需求，密码服务平台提供三种不可否认性服务，分别为签名服务、电子签章服务和时间戳服务。签名服务保障了信息和行为的不可否认性。除进行数字签名保证安全之外，还须确保数据在某一时间(之前)的存在性，时间戳服务采用精确的时间源、高强度高标准的安全机制，为用户提供精确的且不可抵赖的时间戳服务。电子签章服务利用电子签名技术，取代纸面文件签名的程序，保证电子文件的法律效力，为企业和用户提供方便有效的安全保证

● 签名服务

为数据发送方和数据接收方分别签发基于密码技术的数字身份，发送方发送数据时使用密码技术对数据进行签名，接收方收到数据后对数据进行验签，实现数据发送行为的不可否认性。接收方生成响应信息，并使用密码技术对响应信息进行签名，数据发送方收到响应信息并进行验签，实现接收行为的不可否认性。

● 电子签章服务

电子签章是电子签名的一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果，同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性。



云上业务系统客户端访问云上业务系统服务器，请求电子签章，云上业务系统服务器调用电子签章服务完成签章，并保存签章后的电子文件。详细流程如下：

1）电子签章服务为用户证书配置对应的印章；

2）云上业务系统客户端插入智能密码钥匙，根据智能密码钥匙中证书信息访问云上业务系统服务端，获取对应印章；

3）云上业务系统服务器调用电子签章服务获取该证书对应的印章并返回给云上业务系统服务器；

4）云上业务系统服务器返回印章给客户端，客户端使用该印章设置电子签章信息，并向云上业务系统服务器发起电子印章请求，请求信息中包含证书信息、印章坐标位置等信息；

5）云上业务系统服务器调用电子签章服务完成电子文件的签章，并把签章后的电子文件返回给云上业务系统服务器；

6）云上业务系统服务器保存签章后的电子文件，并通知客户端。

时间戳服务

公共资源交易平台技术专用



时间戳是能够保证电子信息时间可信与不可否认的技术手段，时间戳跟签名类似（在签名信息中增加了时间信息），云上业务系统调用时间戳服务，时间戳服务对数据进行打时间戳后返回，云上业务系统进行存储，云上业务系统通过调用时间戳服务的验时间戳接口，对数据进行时间不可否认性验证。

3.2.4.4.2.4.6 **秘钥管理**

系统的安全运营依赖于密钥管理的各个环节，密钥管理包括密钥的生成、备份、恢复、保存、使用及销毁等，其中任何一个环节遭到破坏都将严重危及系统的安全，甚至摧毁整个认证体系，所以密钥的安全管理是保证系统安全运营的重要条件与前提条件。在不同的场景下需要使用不同类型的密钥。

生命周期 / 类型	产生	分发	存储	使用	更新	归档	撤销	备份	恢复	销毁
用户签名私钥	由智能密码钥匙内置硬件芯片产生	智能密码钥匙生成，不涉及密钥分发。	智能密码钥匙内存储。	输入正确的PIN码调用智能密码钥匙中的密	由智能密码钥匙内置硬件芯片更新密钥	不涉及密钥归档。	到期自动撤销。密钥管理员也可以主动撤	不涉及密钥备份。	不涉及密钥恢复。	通过管理工具销毁，也可以在CA系统里进行

公共资源交易平台投标专用
AE2C19CEC7646E1AC9A82C85EA14DB9

				钥。			销。			注销。
用户签名公钥	由智能密钥内硬件产生	密钥由智能密钥生成，不涉及密钥分发。	智能密钥内以证书形式存储。	以证书形式使用。	由智能密钥内硬件更新	以证书形式归档。	到期自动撤销。密钥管理员也可以主动撤销。	以证书形式备份。	以证书形式恢复。	通过管理工具销毁，也可以在CA系统里进行注销。
用户加密私钥	密码服务平台内部生成。	以证书形式分发。	以证书形式存储。	以证书形式存储。	密码服务平台内部更新	以证书形式归档。	到期自动撤销。密钥管理员也可以主动撤销	以证书形式备份。	以证书形式恢复。	在密码服务平台删除后销毁密钥。
用户加密公钥	密码服务平台内部生	以证书形式分发。	以证书形式存储。	以证书形式存储。	密码服务平台内部更新	以证书形式归档。	到期自动撤销。密钥	以证书形式备份。	以证书形式恢复。	在密码服务平台删除后

公共资源交易平台投标专用

	成。						理员也可以主动撤销			销毁密钥。
云上业务系统签名私钥	密码服务平台内部生成。	签名私钥不进行分发。	密码服务平台内部存储。	密码服务平台内部使用。	密码服务平台内部更新	不涉及密钥归档。	到期自动撤销。密钥管理员也可以主动撤销	利用密码服务平台后端密码机的备份制进行备份。	利用密码服务平台后端密码机的恢复机制进行恢复。	在密码服务平台删除后销毁密钥。
云上业务系统签名公钥	密码服务平台内部生成。	以证书形式分发。	以证书形式存储。	以证书形式使用。	密码服务平台内部更新	以证书形式归档。	到期自动撤销。密钥管理员也可以主动撤销	以证书形式备份。	以证书形式恢复。	在密码服务平台删除后销毁密钥。
云上业务系统	密码服务	以证书形	以证书形	以证书形	密码服务	以证书形	到期自动	以证书形	以证书形	在密码服

公共资源交易平台技术专用
AB2619CEC77645E1A62A8B8880A1B83

加密私钥	平台内部生成。	式分发。	式存储。	式存储。	平台内部更新	式归档。	撤销。密钥管理员也可以主动撤销	式备份。	式恢复。	务平台删除后销毁密钥。
云上业务系统加密公钥	密码服务平台内部生成。	以证书形式分发。	以证书形式存储。	以证书形式存储。	密码服务平台内部更新	以证书形式归档。	到期自动撤销。密钥管理员也可以主动撤销	以证书形式备份。	以证书形式恢复。	在密码服务平台删除后销毁密钥。
云上业务系统存储加密密钥	可由密码服务平台内部生成，也可由外部式导	加密密钥存储在密码服务平台内部，不进行分发。	密码服务平台内部存储。	密码服务平台内部使用。	密码服务平台内部更新	不涉及密钥归档。	通过密码服务平台密钥管理功能撤销指定加密	利用密码服务平台后端密码机的备份机制进行备	利用密码服务平台后端密码机的恢复机制进行恢	在密码服务平台删除后销毁密钥。

公共资源交易平台投标专用
ABC19CEC7646E1A62A8B8C8C1083

	入。						钥。	份。	复。	

3.2.4.4.2.4.7 **密码算法**

为确保密码算法的自主可控，降低敏感信息泄露和信息系统遭受攻击的风险，方案中涉及的所有密码产品全部采用国产密码算法，具备商用密码产品认证证书，包括密钥管理系统、服务器密码机、智能密码钥匙、身份认证网关、签名验签服务器、证书认证系统、软件密码模块等。相关算法说明如下：

SM2：是ECC椭圆曲线密码机制，在签名、密钥交换方面不同于ECDSA、ECDH等国际标准，而是采取了更为安全的机制。另外，SM2推荐了一条256位的曲线作为标准曲线。SM2算法主要用于数字签名、签名验证，保证业务数据的完整性、不可否认性。

SM3：是一种密码杂凑算法，此算法适用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。SM3算法主要配合SM2算法使用，完成数字签名和验签业务。

SM4：是一个分组算法，该算法的分组长度为128比特，密钥长度为128比特。加密算法与密钥扩展算法都采用32轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

HMAC-SM3：一种基于Hash函数和密钥进行消息认证的方法，是利用密码学中的散列函数来进行消息认证的一种机制，所能提供的消息认证包括两方面内容：

1）消息完整性认证：能够证明消息内容在传送过程没有被修改。

2）信源身份认证：因为通信双方共享了认证的密钥，接收方能够认证发送该数据的信源与所宣称的一致，即能够可靠地确认接收的消息与发送的一致。

3.2.4.4.2.4.8 **密码应用工作流程**

3.2.4.4.2.4.8.1 对称秘钥分发流程

3.2.4.4.2.4.8.2 USBKEY 管理员分发流程

3.2.4.4.2.4.8.3 USB Key自助分发流程

3.2.4.4.2.4.8.4 移动端预制证流程

3.2.4.4.2.4.8.5 移动端自助发证流程

3.2.4.4.2.4.9 **密码应用改造分工**

项目阶段	开始时间	结束时间	节点内容	责任方	备注
启动阶段			项目启动会	云服务商	
项目规划与方案确认			部署环境及资源调研、准备和设备备货	云服务商	
			部署方案沟通和确认。	云服务商	
			虚拟资源申请	云服务商	
			虚拟资源审批、分配	云服务商	
			云密码机部署	云服务商	
			云密码服务平台安装部署	云服务商	
			软硬件系统配置联调	云服务商	
			云密码服务测试	云服务商	
实施阶段			编写应用系统商用密码应用改造方案	委办局	云服务商提供方案模板
			组织商用密码应用改造方案评审	委办局	
			根据方案进行应用系统密码应用改造	委办局	
			密码应用改造接口对接与测试	云服务商、委办局	
初验			项目初验	云服务商、委办	委办局对平台提供的云密码服务进行初验

公共资源交易平台技标专用

				局	
试运行阶段			产品培训	云服务商	
			产品试运行	云服务商、委办局	
验收阶段			项目验收	云服务商、委办局	委办局对平台提供的云密码服务进行终验

3.2.4.4.3 等保辅助测评专业服务

3.2.4.4.3.1 服务概述

华为云等保安全专业服务面向政府、大型企事业单位提供合规的、全程的、持续的、专家级的信息系统安全测评服务、技术咨询服务、系统定级备案服务、管理制度整改指导服务、差距分析服务、整改方案指导服务等。

根据用户的特定网络环境以及业务运行的具体需求，采用专业化的安全评估工具做为支撑，充分利用华为众多技术专家的专业技能、信息资源以及多年的信息安全实践经验，及时发现信息系统存在的安全隐患，并为用户量身定制整改加固方案，帮助用户实现既定的商业目标，提升信息系统的安全性、稳定性与可靠性，全面提升信息系统安全防护水平。

3.2.4.4.3.2 服务内容

等保安全服务内容包括等保助手和等保测评两个部分，详细的等保安全专业服务内容明细见下表，其中等保助手服务内容主要是下表中安全整改部分，提供差距分析、方案建议、协助整改等服务。等保测评主要是提供测评实施相关的服务内容。

等保助手可以单独提供服务，等保测评不能单独提供服务，需要和等保助手一起提供端到端的等保安全服务。

等保安全服务明细			
阶段	关键服务项	服务项具体描述	输出件/交付成果

项目启动	项目管理	结合华为优秀项目管理实践经验，根据项目实际情况，制定您申请的系统等保的项目计划，并跟进项目的进度；	《项目进度规划表》 《项目沟通矩阵》
定级	协助等保定级与审核	依据《计算机信息系统安全保护等级划分准则》（GB17859-1999） 《信息安全技术 信息系统安全等级保护定级指南》GB/T 22240-2020 等国内相关政策标准 专人协助编写定级报告，可协助约等保定级专家评审；	《定级报告》 《专家评审意见》 等当地网监要求填写的定级材料
备案	备案准备指导	专人指导信息系统等级保护备案表填写；	《备案表》备案证明/备案编号 等当地网监要求填写的备案材料
	测评机构筛选与预约	根据等保要求，在全国范围内（含本地）筛选匹配的等保测评机构，与您共同规划、确定具体的测评时间计划；	《测评申请书》或测评机构所需《调研表》
安全整改（技术部分）	现状分析与差距评估	根据《中华人民共和国网络安全法》、《GB/T22239-2019信息安全技术网络安全等级保护基本要求》等国内相关政策标准，由安全专家现场结合对您申请的系统等级保护的实际情况，同时针对现有的重点信息系统及IT基础架构的合理性进行调研，并根据调研情况进行系统现状分析与差距评估。	《系统安全评估差距分析报告》

公共资源交易平台投标专用

	等保技术条款分析与指导	基于《中华人民共和国网络安全法》、《GB/T22239-2019信息安全技术网络安全等级保护基本要求》等国内相关政策标准，由安全专家现场完成对您申请的系统的等级保护分析评估，包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理方面进行逐条分析，并结合应用系统实际情况，提供相关安全解决方案与部署建议。	《XXX系统等保技术建议书》
安全整改（管理部分）	等保管理制度体系分析与编写指导	对您申请的系统的的实际情况为依据，遵照国家的法律法规和标准规范，参照国际的安全标准和最佳实践，由安全专家现场支撑，依据相应等级信息系统的基本要求和安全目标，设计并指导输出等级化、符合系统特点、融管理和技术为一体的整体安全管理保障体系。	《安全管理保障体系》等文档集
测评实施	测评准备	测评前的材料准备指导。渗透测试应对指导； 预约测评机构测评地点以及测评时间，并与您协商、确认。	《信息采集表》（测评机构输出） 《渗透测试信息表》(测评机构输出）
	测评陪同	测评现场，协助回答测评中问题，解答测评机构提出的疑问。	/

公共资源交易平台技标专用

	测评整改意见应答指导	分析测评机构输出的《整改意见》；按照您申请的系统所在行业的分数要求（如果有），同时协助指导编写“应答报告”；	《整改意见》（含渗透测试报告）（测评机构输出） 《应答报告》
	测评报告跟进	跟进测评机构报告的整理和输出进度；	《测评报告》（测评机构输出）
监督检查	等保相关疑问咨询	完成测评后的一年内，远程解答您所申请的系统相关安全等保问题的咨询；	/

等保助手服务内容

3.2.4.4.3.3 服务流程



入项评估

① 客户提出服务申请

② 华为云评估客户需求

③ 与客户对标，确认本次服务的业务目标及业务范围

授权

① 客户授予华为云实施相关安全专业服务所需相关权限

服务交付

① 完成专业服务所包含的服务内容交付

验收与闭环

① 服务完成后提交书面验收申请，客户给出书面验收通过确认。客户应在等保安全服务交付完毕后【 14 】个工作日内完成验收，如客户未能在前述规定日期内进行验收，则视为验收通过。

② 乙方负责输出项目交付件并自检，合格后提交验收申请

公共资源交易平台投标专用

③ 甲方对交付件进行评审，评审通过后在交付件上签字。若评审有问题，乙方根据评审意见进行整改，重新提交验收申请。

④ 已方收到评审意见后，应 5 个工作日内完成对交付件的修改，并提交修改后的交付件给甲方验收。

⑤ 甲方在收到已方提交的交付件后，应在 5 个工作日内反馈意见给已方，以上过程不应超过 3 次。如果乙方在交付件提交给甲方后的 5 个工作日内尚未收到甲方的书面反馈意见，则该轮提交的交付件将被视为已被甲方接受并作为最终版本验收通过。

3.2.4.4.3.4 责任分工

共同责任

1、 双方商定并确认具体业务目标及范围。

2、 双方完成合同签订。

客户责任

1、 客户指派一位项目负责人协助华为云实施服务。此负责人应负责双方之协调及管理，负责审核、验收华为云提供的服务；

2、 客户必须提供业务系统相关的信息（包括但不限于应用架构、部署架构、资源数量和性能）。

华为责任

1、 华为云需明确此次项目的负责人，因特殊情况导致华为人员变更，需要提前 3 个工作日知会客户，直至项目最终验收完成。

2、 华为云得到客户授权后，授权数据仅限用于等保安全专业服务中涉及的服务内容，不得超出限定范围。

R=责任方Responsibility S=协助方/Support					
序号	业务流程	工作内容	华为	客户	测评机构
1	授权	被服务方提供相关的数据或授权服务	S	R	S

公共资源交易平台投标专用

		方执行相关操作			
2	定级备案	填写《备案表》、《定级报告》等材料	S	R	S
		递交网监审核	S	R	S
3	信息调查表填写与确认	密评机构向被测单位发送信息调查表	S	S	R
		收集信息，梳理云上资源部署情况	S	R	S
		被测方填写信息调查表	S	R	S
		审核信息调查表	S	S	R
4	等保测评	启动现场测评会议	R	S	S
		管理制度测评	S	S	R
		技术条例测评	S	S	R
		结果确认和资料归还	S	S	R
		复测和结果记录	S	S	R
		结果及风险分析	S	S	R
		测评结论形成	S	S	R
5	测评报告编制	编制测评报告电子稿	S	S	R
		电子稿评审	S	S	R
		编制测评报告纸质稿	S	S	R
		纸质稿评审+盖章	S	S	R

等保助手责任分工表

3.2.4.4.4 密评辅助测评专业服务

3.2.4.4.4.1 服务概述

密码安全专业服务面向政府、大型企事业单位提供合规的、全程的、持续的、专家级的信息系统安全测评服务、技术咨询服务、密码建设方案评估、密码改造方案指导服务等。

根据用户的特定网络环境以及业务运行的具体需求，采用专业化的安全评估工具做为支撑，充分利用华为众多技术专家的专业技能、信息资源以及多年的信息安全实践经验，及时发现信息系统存在的安全隐患，并为用户量身定制整改加固方案，帮助用户实现既定的商业目标，提升信息系统的安全性、稳定性与可靠性，全面提升信息系统安全防护水平。

公共资源交易平台技术专用

3.2.4.4.4.2 服务内容

密评安全服务内容包括密评助手和密码测评两个部分，详细的密评安全专业服务内容明细见下表，其中密评助手服务内容主要是下表中方案评估部分，提供差距分析、方案建议、协助整改、方案评估等服务。密码测评主要是提供测评实施相关的服务内容。

密评助手可以单独提供服务，密码测评不能单独提供服务，需要和密评助手一起提供端到端的等保安全服务。

密评安全专业服务明细			
阶段	关键服务项	服务项具体描述	输出件/交付成果
方案评估	用户调研	1、项目需求沟通，对齐项目目标及测评计划	需求沟通会议纪要、项目计划
		2、填写《信息系统调研表》	《信息系统调研表》
		3、调研表分析及评审	
	差距分析	1、密评技术条例满足度分析	《差距分析报告》
		2、密评管理条例满足度分析	
		3、当前现状及差距评估	
	整改方案	1、密评技术条例解读	《整改方案》、《管理制度模板》
		2、指导进行密评技术条例不满足项整改	
		3、密评管理条例解读	
		4、指导进行密评管理条例不满足项整改	
		5、技术及管理层面整改取证指导	
	方案评估	1、密评专家进行方案评估，审查被测系统责任单位的密码应用/密码设计/实施/应急方案	《密码安全方案》（客户输出）《评估报告》
		2、专家评估结论输出	
测评准备	信息收集	密评机构向被测单位发送信息调查表，被测单位安排相关人员完成信息调查表后，被测单位和密评机构对填写完成的信息调	《系统信息采集表》
	信息分析		

		查表进行确认，确保内容准备充分	
	表单准备	密评机构准备现场测评需要的表单、工具	
	工具准备		
方案编制	测评对象	根据了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，以及与此相关的商用密码应用情况，确定本次测评的测评对象	《测评方案》（测评机构输出）
	测评指标	根据已经了解到的被测系统的定级结果，确定本次测评的测评指标	
	测评检查点	测评过程中，确认现场检查的关键安全点，并充分考虑到检查的可行性和风险，最低限度的避免对被测系统，尤其是在线运行业务系统的影响	
	测评方案	完成测评方案编制	
现场测评	测评实施	1、召开现场测评准备会议，交流测评信息、方案、计划，告知风险，资源及测评条件确认，备份确认等信息	《现场测评授权书》（客户提供）
		2、测评委托单位签署现场测评授权书	
		3、根据测评方案及现场测评准备结果，实施测评工作	
	结果记录	汇总现场测评的测评记录	
	结果确认	测评过程中发现的问题进行确认	
	资料归还	测评机构归还测评过程中借阅的所有文档资料	
分析与报告编制	结果判定	根据现场测评情况初步判定单元测试结果	《整改意见》《应答报告》《测评报告》（测评机构输出）
	整体测评	对测评结果汇总分析，形成测评结论	
	风险分析	对测评结果记录的密码应用安全问题分析，并与评估系统单位进行问题反馈	
	报告编制	测评单位对密码应用安全问题进行相应的	

公共资源交易平台投标专用

		整改，经最终整改确认后，编制完成测评报告	

密评助手服务内容

3.2.4.4.4.3 **服务流程**



入项评估

① 客户提出服务申请

② 华为云评估客户需求

③ 与客户对标，确认本次服务的业务目标及业务范围

授权

① 客户授予华为云实施相关安全专业服务所需相关权限

服务交付

① 完成专业服务所包含的服务内容交付

验收与闭环

① 服务完成后提交书面验收申请，客户给出书面验收通过确认。客户应在等保安全服务交付完毕后【 14 】个工作日内完成验收，如客户未能在前述规定日期内进行验收，则视为验收通过。

② 乙方负责输出项目交付件并自检，合格后提交验收申请

③ 甲方对交付件进行评审，评审通过后在交付件上签字。若评审有问题，乙方根据评审意见进行整改，重新提交验收申请。

④ 已方收到评审意见后，应 5 个工作日内完成对交付件的修改，并提交修改后的交付件给甲方验收。

甲方在收到已方提交的交付件后，应在 5 个工作日内反馈意见给已方，以上过程不应超过 3 次。如果乙方在交付件提交给甲方后的 5 个工作日内尚未收到甲方的书面反馈意见，则该轮提交的交付件将被视为已被甲方接受并作为最终版本验收通过。

公共资源交易平台投标专用

3.2.4.4.4.4 责任分工

共同责任

1、 双方商定并确认具体业务目标及范围。

2、 双方完成合同签订。

客户责任

1、 客户指派一位项目负责人协助华为云实施服务。此负责人应负责双方之协调及管理，负责审核、验收华为云提供的服务；

2、 客户必须提供业务系统相关的信息（包括但不限于应用架构、部署架构、资源数量和性能）。

华为责任

1、 华为云需明确此次项目的负责人，因特殊情况导致华为人员变更，需要提前3个工作日知会客户，直至项目最终验收完成。

2、 华为云得到客户授权后，授权数据仅限用于密评安全专业服务中涉及的服务内容，不得超出限定范围。

R=责任方Responsibility S=协助方/Support					
序号	业务流程	工作内容	华为	客户	测评机构
1	项目管理	指定专家参与交付，制定项目计划	R	S	/
2	用户调研	需求沟通	R	S	/
		信息收集与分析	S	R	/
3	差距分析	密评技术条例分析	R	S	/
		密评管理条例分析	R	S	/
		现状分析与差距评估	R	S	/
4	整改方案	整改建议方案输出	R	S	/
		不满足项整改	S	R	/
5	方案评估	输出密码安全方案	S	R	/

公共资源交易平台投标专用

		密评专家进行方案评估	R	S	/
		专家评估结论输出	R	S	/
6	授权	被服务方提供相关的数据或授权服务方执行相关操作	S	R	S
7	测评准备	密评机构准备现场测评需要的表单、工具	S	S	R
8	信息调查表填写与确认	密评机构向被测单位发送信息调查表	S	S	R
		收集信息，梳理云上资源部署情况	S	R	S
		被测方填写信息调查表	S	R	S
		审核信息调查表	S	S	R
9	密评方案编制	根据信息调查表，编制密评方案	S	S	R
		方案评审	S	R	S
10	现场测评	启动现场测评会议	R	S	S
		现场测评和结果记录	S	S	R
		结果确认和资料归还	S	S	R
		现场复测和结果记录	S	S	R
		分析评估结果	S	S	R
		风险分析	S	S	R
		测评结论形成	S	S	R
11	测评报告编制	编制测评报告电子稿	S	S	R
		电子稿评审	S	S	R
		编制测评报告纸质稿	S	S	R
		纸质稿评审+盖章	S	S	R

密评助手责任分工表

3.2.5 云平台与监管接口对接方案

为了满足云监管平台的建设，我方能承诺在中标后提供接口定制化开发服务，参与云监管平台、云安全运维与云服务商平台间监管接口规范的制定、开发，配

公共资源交易平台投标专用

合适配和联调等工作。

3.2.5.1 体系架构



在提供标准云管理服务平台的基础上，按照面向用户的需求，定制的政务云资源管理监控平台。以现有的产品接口服务为通道，二次开发更为适应用户使用的管理门户。

定制的系统模块是对于原有服务平台的优化，是贯彻面向用户的应用软件交互体验设计理念的最佳实践方式，从更本上解决用户对于高端云产品系统的使用体验和使用门槛的问题。

3.2.5.2 基本要求

为了保证系统的完整性和健壮性，系统接口应满足下列基本要求：

接口应实现对外部系统的接入提供企业级的支持，在系统的高并发和大容量的基础上提供安全可靠的接入；

提供完善的信息安全机制，以实现对信息的全面保护，保证系统的正常运行，应防止大量访问，以及大量占用资源的情况发生，保证系统的健壮性；

提供有效的系统的可监控机制，使得接口的运行情况可监控，便于及时发现错误及排除故障；

保证在充分利用系统资源的前提下，实现系统平滑的移植和扩展，同时在系统并发增加时提供系统资源的动态扩展，以保证系统的稳定性；

在进行扩容、新业务扩展时，应能提供快速、方便和准确的实现方式。

公共资源交易平台投标专用

3.2.5.3 接口技术架构



统一接口架构设计

3.2.5.4 接口标准体系与规范

ITSS 体系接口技术要求

信息接口技术要求 从标准实施的角度出发，接口仅涉及数据集成接口，对不同层次间的 集成数据提出了要求，没有要求具体的实现方法。

接口包括两个层次：

监控管理与过程管理之间的信息交互；

过程管理向决策支撑的信息传递。

监控管理与过程管理间接口对三种接口作了规范：双向配置接口、从 监控到过程的单向告警和性能接口。

过程管理与决策支撑之间对十种接口作了规范：

（1）事件信息传递接口

（2）问题信息传递接口

（3）变更信息传递接口

（4）发布信息传递接口

（5）服务级别信 息传递接口

（6）可用性信息传递接口

（7）能力信息传递接口

（8）持续性信息传递 接口

（9）业务关系信息传递接口

（10）服务台信息传递接口

（11）接口安全要求

为了保证系统的安全运行，各种接口方式都应该保证其接入的安全性。

接口的安全是系统安全的一个重要组成部分。保证接口的自身安全，通过接口实现技术上的安全控制，做到对安全事件的"可知、可控、可预测"，是实现系统安全的一个重要基础。

公共资源交易平台技标专用
AE2C1...7646E1A62A8BC88EA14DB9

根据接口连接特点与业务特色，制定专门的安全技术实施策略，保证接口的数据传输和数据处理的安全性。

系统应在接入点的网络边界实施接口安全控制。

接口的安全控制在逻辑上包括：安全评估、访问控制、入侵检测、口令认证、安全审计、防恶意代码、加密等内容。

3.2.5.5 **统一接口设计**

提供各种标准和开放的接口，支持与其它各类系统的集成。主要支持的系统包括邮件与短信平台；监控平台，覆盖市面主流的监控平台；统一认证系统如 AD 和 LDAP；与企业门户网站或者 OA 的集成等。

统一接口设计：包含了标准的接口规范与具体的统一云管平台的接口服务的配置与开发（包含：封装的云运营运维系统的北向接口、统一应用、服务、管理与监控接口），提供统一云管平台沟通两个云服务供应商提供的云平台运营运维系统的需求，同时为日常运维和运营过程中产生的新的管理与保障需求，提供对应的开放性的 API 接口，实现可扩展的定制开发服务，以满足不断增长的运维管理需求。

3.2.5.6 **接口通讯方式**

接口基本采用了同步请求/应答方式、异步请求/应答方式、会话方式、广播通知方式、事件订阅方式、可靠消息传输方式、文件传输等通讯方式：

（1）同步请求/应答方式

云用户端向服务器端发送服务请求，云用户端阻塞等待服务器端返回处理结果；

（2）异步请求/应答方式

云用户端向服务器端发送服务请求，与同步方式不同的是，在此方式下，服务器端处理请求时，云用户端继续运行；当服务器端处理结束时返回处理结果；

（3）会话方式

云用户端与服务器端建立连接后，可以多次发送或接收数据，同时存储信息的上下文关系；

（4）广播通知方式

由服务器端主动向云用户端以单个或批量方式发出未经云用户端请求的广

播或通知消息，云用户端可在适当的时候检查是否收到消息并定义收到消息后所采取的动作；

（5）事件订阅方式

云用户端可事先向服务器端订阅自定义的事件，当这些事件发生时，服务器端通知云用户端事件发生，云用户端可采取相应处理。事件订阅方式使云用户端拥有了个性化的事件触发功能，极大方便了云用户端及时响应所订阅的事件；

（6）文件传输

云用户端和服务器端通过文件的方式来传输消息，并采取相应处理；

（7）可靠消息传输

在接口通讯中，基于消息的传输处理方式，除了可采用以上几种通讯方式外，还可采用可靠消息传输方式，即通过存储队列方式，云用户端和服务器端来传输消息，采取相应处理。

3.2.5.7 **传输控制要求**

传输控制利用高速数据通道技术实现把前端的大数据量并发请求分发到后端，从而保证应用系统在大量云用户端同时请求服务时，能够保持快速、稳定的工作状态。

系统应采用传输控制手段降低接口网络负担，提高接口吞吐能力，保证系统的整体处理能力。具体手段包括负载均衡、伸缩性与动态配置管理、网络调度等功能：

（1）负载均衡

为了确保接口服务吞吐量最大，接口应自动地在系统中完成动态负载均衡调度；

（2）伸缩性与动态配置管理

由系统自动伸缩管理方式或动态配置管理方式实现队列管理、存取资源管理，以及接口应用的恢复处理等；

（3）网络调度

在双方接口之间设置多个网络通道，实现接口的多数据通道和容错性，保证当有一网络通道通讯失败时，进行自动的切换，实现接口连接的自动恢复。

公共资源交易平台投标专用

3.2.5.8 **可扩展性接口**

（1）应用、服务的可扩展性接口

为使系统具有较好的开放性和可扩展性，需要基于可开放的系统平台，遵循业界标准，并提供开放、灵活的信息交互及开发接口，方便扩展管理功能。并且支持第三方厂商的应用集成，为后续相关产品的选型提供更高的灵活性。

全面支持 XML、SOAP、Web Service、LDAP 等当前受到普遍支持的开放标准，这保证了本方案能够与其它平台的应用系统、数据库等相互交换数据并进行应用级的互操作和互连性，为平台在应用、服务层面的可扩展性奠定基础。

（2）管理、监控的可扩展性接口

在系统管理、监控层面提供可扩展性接口，例如:

1）可扩展的资源管理接口

通过此接口，对云内所有资源，如网路、存储、服务器、软件、数据库等，进行增加、删减、修改、配置及自动化发现。

2）可扩展的身份认证接口

身份认证机制可扩展，允许接入今后新建的应用系统服务，并允许把已有的应用系统集成起来。这样可以大大简化用户界面，用户可采用统一认证方式，使用多种服务。

3）可扩展的计费接口

云平台可提供开放的计费接口，供业务支撑系统使用。计费信息可包括：采集时间、账户标识、业务代码、费用类型、服务时候用时长、用户标识等信息。

4）可扩展的状态报表接口

云平台可提供开放的状态接口，将云管理平台采集到的用户使用数据以多种方式转发给统一云管平台系统使用，如定时传输、准时异步传输、批量传输等。

3.2.5.9 **接口设计**

参考的接口技术文档细项设计表

序号	接口类型	接口分类
1	认证接口（登录认证、认证校验、登出认证、分权分与校验、当前登录用户密码认证、注销当前登录用户、根据 toolId、随机数获取 TOKEN）	服务管理 数据共享

公共资源交易平台投标专用

2	工单接口（工单获取、工单调用、工单反馈、工单分配、工单下发、工单修改、工单删除）	工单管理
3	服务台账（工单获取、运维工单执行、运营工单执行、服务人工折算、工单记录、工单反馈）	服务管理
4	计量（网络流量获取、获取计算资源计量表、获取服务资源计量表、主机监控获取、数据库监控获取、资源归属信息获取） 计费（计费公式获取、计算折扣、服务目录获取、修改单价、修改折扣、获取协议 SLA 公式等）	计量计费
5	资源对象接口（获取资源对象类型列表、获取对象属性列表、获取指定类型对象资源列表、获取指定对象详情、增加资源对象、修改资源对象、删除资源对象、获取历史资源变更列表）	资源监控
6	告警时间接口（获取当前告警列表、获取告警详情、获取告警状态、获取历史告警列表、获取告警字典详情、产生告警、告警清除、统计当前告警数量、告警清除扩展接口、第三方上报告警、修改告警对象/级别/备注、修改告警状态、获取事件列表）	服务管理
7	性能数据接口（获取实时性能数据、获取历史性能数据、获取性能 KPI）	资源管理
8	拓扑接口	资源管理
9	订阅接口（发送邮件、发送短信、订阅通知、取消订阅）	服务管理
10	日志接口（写操作日志、系统日志、安全日志）	服务管理
11	公告接口（获取公告、公告推送、公告作废）	公告管理
12	消息接口（消息接收、消息推送、消息延迟、消息分发）	消息管理
13	CA 证书（CA 证书验证-模块级/系统级、CA 证书授权、CA 证书作废）	CA 接口

3.2.5.10 **任务流转接口**

让任务流程化的流动起来，可推动执行力，方便各层领导安排任务、跟踪监

公共资源交易平台技标专用

督任务以及最终评估完成结果。

在日常工作中，具体的任务和实物错综复杂，常常容易被遗漏、拖延或是在低效的状态下完成。任务流转接口的设计就是为了更加方便的分摊任务、更加专业的分配任务、更加实时的监控任务。

1、任务可以在团队内部依据个人待办任务情况、个人业务熟悉度来流转。

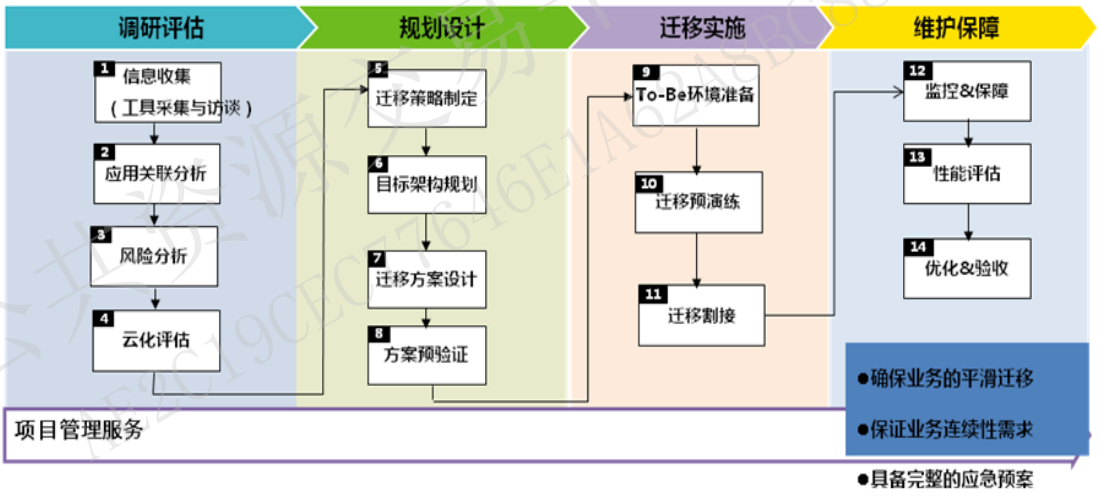
2、任务完成进度显示，任务流转接口可以获取每个团队成员正在处理任务的进度情况，并以之为任务自动再分配计的依据。

3、任务分类显示，可以根据任务的内容关键字，将任务分配为若干类别。针对每个类别内任务的排队情况，进行任务再分配。

4、自动汇总任务情况，形成统计分析报告，增加任务数据的可读性。不但团队成员可以方便自我管理和检查，提高工作效率，各层的管理者也能用最搞笑的方式进行管理。

3.2.6 迁移上云方案

根据政府的需求，移动公司提供服务内容如下：



阶段	NO.		说明
调研评估	1	信息收集	使用工具或业务调研表，了解业务系统 IT 现状
	2	应用关联分析	根据调研表分析整个业务关联关系及业务中断造成影响
	3	风险分析	根据调研表分析整个迁移风险情况，作为规划设计中的依据

	4	云化评估	根据业务调研以及分析结果。制定整体的业务迁移策略
规划设计	5	迁移策略制定	制定业务迁移整体计划，细化各子系统的详细计划，包括：环境准备，迁移演练、系统备份、迁移实施、业务切换
	6	目标架构规划	根据不同的业务特点以及需求定制业务迁移解决方案
	7	迁移方案设计	针对整个业务迁移风险情况制定相应的应对措施及计划
	8	方案预验证	在后台数据中心部署业务迁移工具，对业务迁移工具进行测试，验证并完善迁移方案，开始正式业务切换宣传
迁移实施	9	To-Be 环境准备	根据规划设计方案，在目标端完成系统、数据库、存储和网络环境安装配置。测试目标端环境，并测试源端和目标端网络连接通讯成功
	10	迁移演练	迁移前进行一次全面的数据备份，以保证数据的可用性和完整性，按照迁移规划及业务系统、数据库进行数据同步配置。协助客户按照迁移计划及方案对业务系统进行迁移切换演练测试（可选）
	11	迁移割接	协助客户按照迁移计划及方案对业务系统进行正式迁移切换
维护保障	12	监控&保障	为了保证迁移后系统的高效稳定运行。必要对迁移后的系统进行一段时间的监控。并对迁移后的系统进行评估优化。保证迁移后，业务持续平稳运行。
	13	性能评估	根据性能基线，评估迁移后系统、数据库运行性能情况，评判是否满足业务运行性能要求。

公共资源交易平台招标专用

验收	14	优化&验收	项目验收。如果存在性能问题，怎进行系统、数据库层面的优化，或推动业务层面进行 SQL 等方面的优化。最终达到运行性能要求。

3.2.6.1 **评估分析**

3.2.6.1.1 信息收集

收集的内容可包括以下几个方面：

1. IT硬件资产：了解客户目前业务系统的硬件信息，例如服务器类型、磁盘阵列类型等等，为云迁移提供原始输入信息。
2. 系统性能参数：收集客户现行业务及IT设备具体信息，为客户云迁移可行性分析、云平台容量规划和云迁移提供最直接的信息。
3. IT系统配置：通过了解客户目前配置和性能情况，评估迁移至我司云平台上性能情况，作为业务发放和资源配置的参考基准。
4. 业务流程：要清楚客户业务流程，这样才能根据客户实际情况制定迁移方案。
5. 业务&IT联系：从IT的角度看，系统的优先级是怎样的。
6. IT网络配置：了解客户目前组网情况。重点关注网络带宽信息。
7. 客户其他要求：详细了解客户对整个云迁移的特殊需求。

交付输出件：

- 《xx 公司 xx 业务信息收集表》

3.2.6.1.2 迁移可行性分析

1. 兼容性分析：参照虚拟化平台和迁移工具的兼容性列表评估业务虚拟化部署的可行性；
2. 性能分析：对采集的原业务系统的运行负载数据（如CPU、内存使用率、网络IO等）进行计算评估，或根据POC测试验证的结果，判断业务系统是否适合进行虚拟化部署；
3. 业务分析：分析客户业务现状，包括客户服务器类型、使用的其他虚拟化平台、服务器操作系统类型、业务种类、业务重要性、业务部署模式、业务是否24小时运行、业务之间的关联性等；

交付输出件：

- 《xx 公司 xx 云迁移可行性分析报告》

3.2.6.2 规划设计

规划设计主要包括迁移流程、方案和应急预案的制定。输出方案均要经过相关团队的评审（客户、业务系统维护团队、迁移实施团队等）。云迁移以专业服务团队为主实施，业务验证和切换、关联变更以客户工程师为主实施。

对客户可迁移云迁移制定详细的实施方案。迁移方案主要内容如下：

表：迁移方案主要步骤

编号	步骤	编号	步骤
1	迁移方法选定	9	迁移时间和停机时间安排
2	迁移工具选型	10	云迁移
3	数据备份	11	数据同步
4	迁移测试环境准备	12	验证业务
5	迁移工具安装	13	业务割接
6	云迁移演练	14	业务再次验证
7	正式迁移环境准备	15	关联系统的变更
8	迁移人员安排	16	风险应对及失败回退

交付输出件：

- 《xx公司xx云迁移实施方案》

3.2.6.3 实施迁移

3.2.6.3.1 迁移演练

迁移演练可以视为迁移实施方案的一部分，在正式实施迁移前根据需要进行迁移的演练。

1. 迁移实施团队可以通过演练提升操作技能。
2. 增加多团队的配合度，提升效率。
3. 提前发现迁移方案可能存在的问题，如网络不通、带宽限制等。

公共资源交易平台投标专用

3.2.6.3.2 方案实施

根据既定的迁移方案，结合迁移演练（可选）的结果，在确定正式的项目启动时间后进行迁移方案实施，主要包含以下步骤：

表：方案实施主要步骤

编号	步骤	编号	步骤
1	迁移环境准备	6	业务割接
2	迁移工具安装	7	业务再次验证
3	云迁移	8	关联系统的变更
4	数据同步	9	风险应对及失败回退
5	验证业务		

3.2.6.4 优化验收

3.2.6.4.1 迁移验收

根据客户需求制定验证标准，配合客户进行业务和功能测试，输出详细的云迁移验收报告。主要工作内容如下：

1. 验证方案设计。项目背景、系统概述、验证标准、验证内容。
2. 验证方案交流与确认。与客户就测试方案进行交流，得到客户确认。
3. 验证方案实施。每次云迁移完成后，配合客户进行业务验证和测试，确保验证通过。
4. 验证报告提交。将验证报告提交给客户确认。
5. 交付输出件：《xx 公司 xx 云迁移验收报告》。
6. 在验证时须注意以下几点：
   (1) 提前确认验证时间、验证方式、验证内容、参加验证的人员等。
   (2) 验证方案在交付设计阶段完成初稿，根据现场集成联调的情况做相应调整，到内部项目组和技术专家组评审，确保方案的准确和完整。

公共资源交易平台技术专用

(3) 验证过程中因为不可抗力等因素影响到验收指标的，如突然产生的外界干扰等，应该冷静处理，以事实和数据说话。

(4) 避免多次验证测试。

(5) 对于需要进行验证测试的专业服务交付项目，应尽量在交付实施过程中完成技术指标的测试，双方签字确认的数据在得到用户许可后，可以作为验证的测试数据使用。验证时要求服务经理、行销工程师参加。

(6) 验证过程中的每一个迁移完成的业务系统都必须有用户签字；

(7) 验证通过后，移交项目验收资料等文档给用户；

3.2.6.4.2 迁移资料归档

迁移项目实施过程中总结的问题经验、项目材料都要以文档的方式积累。

交付输出件：

1. 《xx 公司 xx 业务信息收集表》
2. 《xx 公司 xx 云迁移可行性分析报告》
3. 《xx 公司 xx 云迁移实施方案》
4. 《xx 公司 xx 云迁移验收表》

3.3 项目实施方案

3.3.1 概述

3.3.1.1 方案概述

根据对南阳市人民政府政务云项目需求的理解，河南移动将利用自身雄厚的技术力量为该项目提供优质服务。同时，河南移动将选择公司的原厂服务作为在技术保障体系上的补充，圆满完成本项目的安装调试、技术支持等相关服务。下文将从以下个方面阐述中国移动通信集团河南有限公司南阳分公司在南阳市人民政府政务云项目中的工程实施建议：

（1）项目实施策略；

（2）项目组织结构图与责任；

（3）项目实施流程；

（4）项目管理流程；

公共资源交易平台投标专用
AE2019CEC77646E1A62A8BC88EA14DB9

（5）项目管理 IT 系统与数据库。

3.3.1.2 工程施工方式概述

河南移动将派遣专业项目经理及技术人员团队，按该项目和河南移动商定的日期完成合同设备的安装、调试，并对该项目维护人员进行现场技术指导和培训。在安装过程中，该项目负责整个工程的管理和协调，并且指定技术人员负责该工程的配合和相应的协调工作，并安排适当数量的辅助人员，配合河南移动技术人员从事安装、搬运及其它辅助工作。

3.3.2 服务体系的标准化

3.3.2.1 项目团队的标准化建设

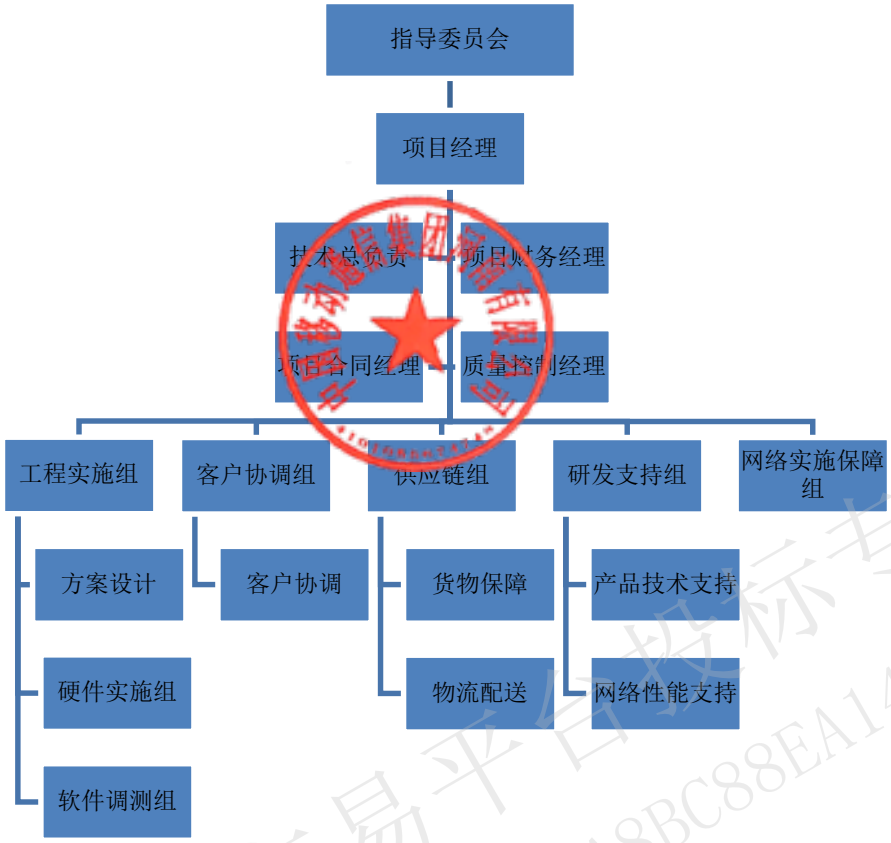
针对本工程质量要求高、工程体量大、专业系统复杂、操作性强等特点。为保证该项目此项目圆满交付，河南移动拟派项目经验丰富的项目经理担任本工程的驻现场项目经理，负责各种重大问题的处理及重要关系的协调，全面调配我方的技术人员、设备工具、现场采购等资源，使项目资源实现最优化配置，为本工程的顺利实施提供全力支持和保障。

参考河南移动丰富的项目交付经验，结合本工程的具体内容和特点，组建“交付项目组”，严格推行“项目经理责任制”和“项目成本核算制”，严格执行科学的项目实施管理流程和要求，项目组代表我公司全面履行对业主的合同。

按照“结构合理、精干高效、分工协作”的原则，项目组设项目经理、项目技术负责人等项目领导岗位并配备数量足够、专业齐全、大型项目施工管理经验丰富、年富力强、高素质的施工管理及技术人员，对项目施工实施全过程、全方位的“四控制”（即进度、质量、成本、安全控制）、“三管理”（即现场（要素）、信息、合同管理）和“一协调”（即组织协调），确保实现项目管理的各项目标。

公共资源交易平台招标专用

3.3.2.1.1 项目实施组织结构图



3.3.2.1.2 项目实施组职责分工

3.3.2.1.3 指导委员会

指导委员会的职责是跟踪项目以及在需要时启动意外情况的支持措施来履行对该项目的承诺和保证项目成功实施。

指导委员会的主要成员包括：

该项目高层领导、工程管理负责人

河南移动高层领导、工程管理负责人

3.3.2.1.4 项目管理团队

该项目应由客户和我司的项目经理组成联合项目管理团队，总体负责项目的成功实施。联合的项目管理团队可以最大程度的做到信息充分共享，沟通顺畅，减少因配合失误造成的工程延误等问题。

项目管理团队的职责如下：

在解决方案的设计、交付、安装与测试方面，履行合同义务与要求。

公共资源交易平台投标专用

代表河南移动与该项目的工程管理人员接口，协调本合同工程交付相关问题。

进行项目规划、控制与汇报。

维护交付的订货至交货时间。

达到议定的目标。

确保工作高质量完成。

项目副经理或其他支持人员将被任命，以协助项目经理在项目实施期间处理项目事宜。

项目经理向项目指导委员会汇报工作。

3.3.2.1.5 工程实施组

工程实施组负责项目实施。该组主要包括三部分：方案设计、硬件安装、软件调测。

根据项目范围，负责编制工程现场实施方案、计划和人力资源计划；

直接负责工程的进度、安全、质量和成本，并将存在的问题和进度信息及时汇报给项目经理；

管理各模块工程的实施流程、验收流程与验收文档，确保符合项目的各项要求；

负责各模块工程的及时交付，并与项目经理共同负责工程安装督导的培训、管理和绩效评估；

在工程实施过程中协调和反馈客户、合作方和各责任主体之间的关系；

协调解决施工过程中的技术问题。

3.3.2.1.6 客户协调组

负责与客户接口总体协调客户相关配套准备事宜，推动客户按项目主计划要求完成客户责任的相关工作；

负责推动项目相关的其它客户、友商、最终用户（尤其是 VIP 用户）、站点业主对项目实施中的配合；

及时向项目组汇报客户责任的相关工作结果。

3.3.2.1.7 质量保证组

质量保证组重点是要确保本工程项目的实施质量，其主要职责包括但不限于：

公共资源交易平台技标专用

根据我司和该项目的评判标准，制定本工程项目的质量评判标准。

制定本工程项目的质量保证计划和质量控制计划。

定期进行抽样和现场检查。

及时向项目经理汇报意外事故，并跟踪事故处理。

3.3.2.1.8 供货保证组

为确保设备的准时和安全交付，我司成立了自己的供货保障组，以监督和控制设备交付。该组负责：

按照项目需求与交付界面，制定满足项目交付需求的货物供应方案，包括合理分批、包装、运输方式、到货、分货要求等详细解决方案；

按照项目要求，参与发货到货计划与安装计划的集成，确保满足国网信通需求与项目交付节奏的货物需求，并保持发货批量经济，仓库存量合理流转，减少仓存积压；

3.3.2.1.9 研发支持组

根据项目主计划，负责计划和组织资源现场保障项目的技术实施活动；

负责产品解决方案的产品技术评审，确保解决方案的可实施性；

负责产品、版本问题以及新需求的现场解决和调研。

3.3.2.1.10 网络实施保障组

根据项目设计方案及实施计划，负责计划和组织网络部分实施保障等技术活动。

3.3.2.2 项目管理的标准化流程

项目管理流程包括监督、信息收集与分析以及工程管理：

（1）监督、收集与分析

通过使用常用评审点（包括项目组和正式评审）监督和控制项目进度。

巩固持续报告的基础便于管理，并提供合适的决策信息。

（2）管理

协调管理项目组资源，维护信息流程并控制项目交付的质量。管理控制发生的变更，并解决项目过程中出现的问题。代表项目组进行承诺，并采取恰当措施达到该项目的期望值。

公共资源交易平台投标专用

3.3.2.2.1 进度管理

本步骤的目标是监控项目进度，以便项目按照工期计划表要求进行。我司 X 将收集实际工作进展信息，分析造成偏差的原因，并采取相应的改进措施。

在项目开始阶段将分配任务，并获取制定项目计划所需的信息。项目组定期举行会议，评估项目工期进度表并审核已完成事宜。确保所有已讨论的任务均已确定，并指派给合格的项目成员。应采取恰当措施激励项目组，并确保项目组可对项目结果进行承诺。

按照下列步骤制定主要项目计划：

建立工作分解结构（WBS）

制定项目基线时间表

确定项目计划的支持单元

我司 X 项目经理使用 Microsoft Project 软件或 RPM 项目管理工具并通过设置下列信息以控制进度计划表：

里程碑和评审点

任务间的联系

产生关键影响的关键依赖点

质量控制活动

资源配置与共享

基准起止日期

预计起止日期

实际起止日期

该计划将定期更新，列出期间出现的偏差，确定造成偏差的原因，并采取改正措施。

相关数据将在项目组内并与该项目共享。

3.3.2.2.2 沟通管理

本工程项目涉及的模块较多，相关接口复杂，环环相扣，沟通不畅将导致进度受阻、管理部门缺乏相关信息而无法正确决策以及项目团队难于协调完成全盘工程计划等。

为尽可能避免上述问题的发生，我司 X 将会采取以下应对措施：

公共资源交易平台投标专用

分析本工程项目干系人情况，识别出关键干系人，制定详细的沟通矩阵。

分析项目各干系人对信息的需求，提前制订沟通计划，保证各方的信息需求得到满足。

在流程演练中验证沟通计划。

制定规范的日报、周报和月报制度。

加强总项目组与各分小组的内部沟通，召开每日例会和每周总结会，做到项目实施中的信息共享。

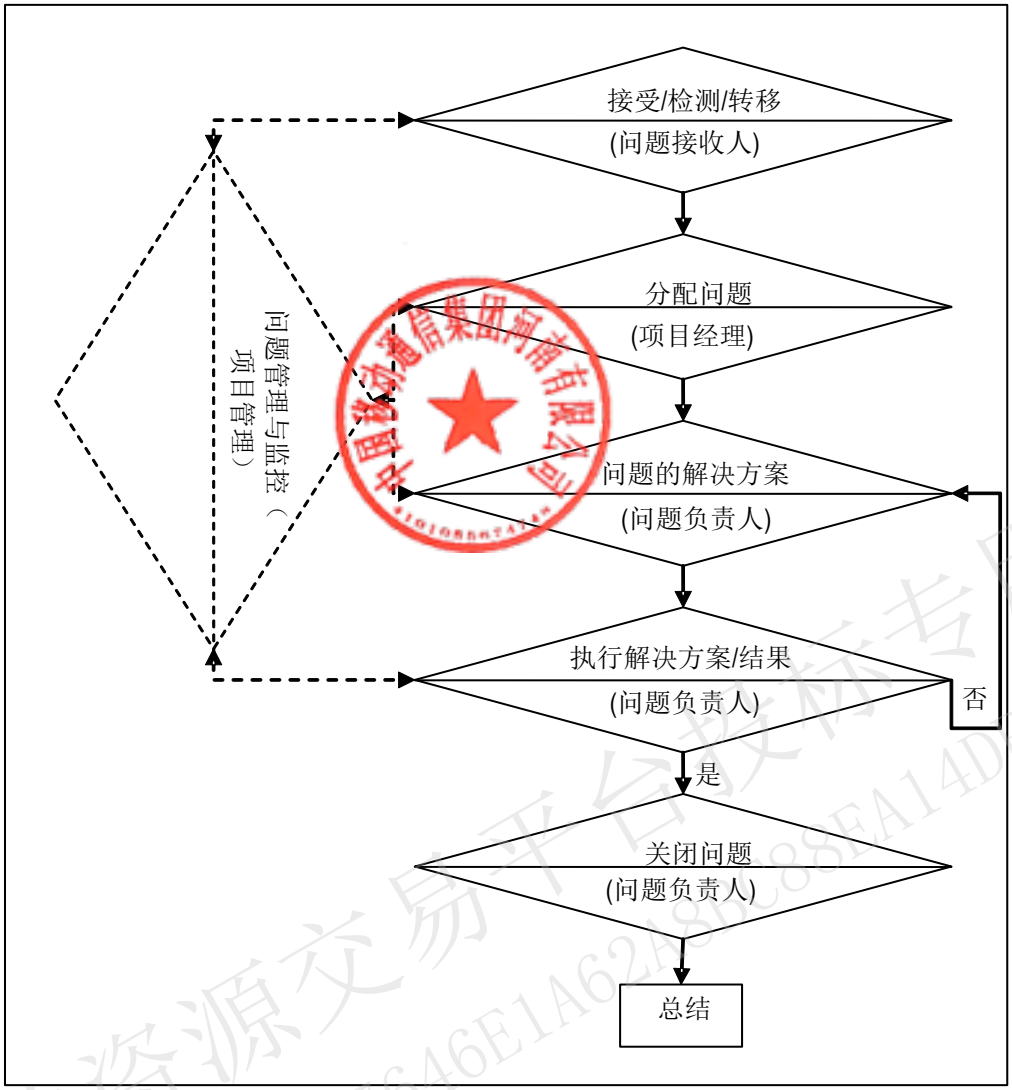
组织召开工程进展汇报和问题推动相关会议。

制作和不断更新项目联系人员表。

3.3.2.2.3 问题管理

此处的问题是指项目中出现但不一定会破坏整个项目的问题。问题可能源自项目组织内部和影响项目的环境。我司将尽量高效地评估并处理出现的问题。问题通常会遗留下来，即使预计已经得到了解决，因此必须跟踪问题直至完全解决。该步骤的目标是解决影响项目成功的问题，以便项目按计划进行。

公共资源交易平台技术专用
AE2C19CEC77646E1A62A8BC8CFA1



任何项目管理问题都将向项目经理汇报，并被记录在“项目问题日志”中。汇报人员将确保所有问题均向恰当级别的负责人汇报以作解决或决策。

3.3.2.2.4 变更管理

变更请求可能来自各个方面。请求方将描述变更请求并提供合理解释，确认替换方案及其对项目的相关影响，并提出建议。建议将提交给恰当授权级别人员以作决策。

对合同的任何变更都必须以书面形式作出。

3.3.2.2.5 文档控制

作为项目管理的重要组成部分，项目文档管理贯穿从项目开工到关闭阶段的整个过程。 我司团队建立的系统可以清晰有效地管理和控制所有文档，确保文档正确可用。

公共资源交易平台技术专用
AE2C1534E27646E1A624B88EA14DB9

3.3.2.2.6 货物管理

负责合同货物管理和控制，确保发货计划满足整个项目计划要求。

3.3.2.2.7 特殊情况处理

特殊情况是指对项目产生重大影响并通常由项目管理团队处理的问题。该步骤的目标是使我司在项目偏离预定轨道时能够采取纠正措施，从而使项目仍可在获得该项目高满意度的情况下成功完成。特殊情况管理的目标是将对项目的影响降至最低，并征得项目组内部所有部门和该项目的一致同意。

3.3.2.2.8 问题升级流程

当确定项目管理团队有必要将关键问题升级至指导委员会时，可能还应要求客户参与，以确保项目的成功交付。 升级报告由项目经理撰写，通常包括下列信息：

对项目的影响；

问题的相关信息；

经检查的选项；

推荐执行的计划/措施。

指导委员会应征求所有方的一致认可并正式决策。

3.3.2.2.9 健康与安全控制

为加强该项目项目现场安全生产监督和管理，防止项目现场施工安装督导及配合、调试测试、开通运营期间发生安全事故，保障职工生命和企业财产安全，确保南阳市政府电子政务云项目顺利实施，保障雇员的安全、福利和健康。

项目组将采取一切必要措施，保证人身财产安全。严格遵守各项安全生产制度，正确使用个人防护用品。及时汇报各种安全隐患、事故，现场采取必要应对措施。特种作业，持证上岗；一般作业，培训上岗。决不酒后上岗，带病工作。

为此，项目组制定《安全管理手册》、《安全条例》，要求项目组成员签署《安全承诺书》，现场施工完成《现场 EHS 遵从性检查 checklist》、《项目 EHS 管理必要活动 CHECKLIST》检查，目标是创建安全健康的工作环境。

3.3.2.2.10 项目管理 IT 工具

河南移动已经建立业界先进的项目管理 IT 工具系统，实现对工程项目的 IT

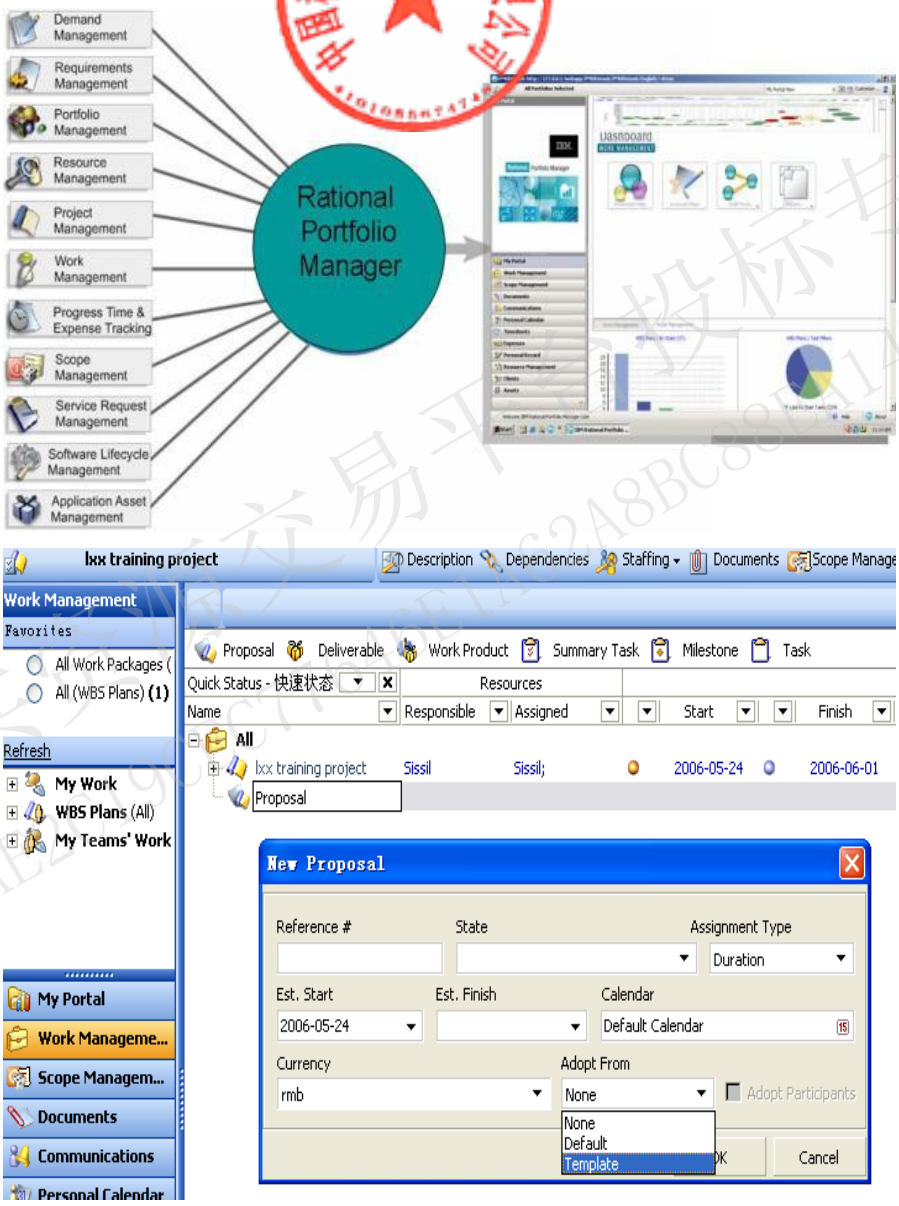
公共资源交易平台投标专用

化、规范化、集成化的管理，极大提升了项目运作的效率和质量。

Rational Portfolio Manager (RPM)

我司使用综合的项目管理 IT 工具 RPM（Rational Portfolio Manager）。该工具在 IBM 已被证明为最佳实践。 RPM 基于互联网，并安装在受保护的高速服务器中。

RPM 是可扩展的完善工具，将项目管理的各个方面综合于一个统一平台，并提供可配置的仪表板以作分析。



RPM 有助于项目组将许多主要流程自动化以便管理。

对于项目组，该工具可：

持续计划、执行和管理项目

在正确的时间匹配合适技能到合适工作

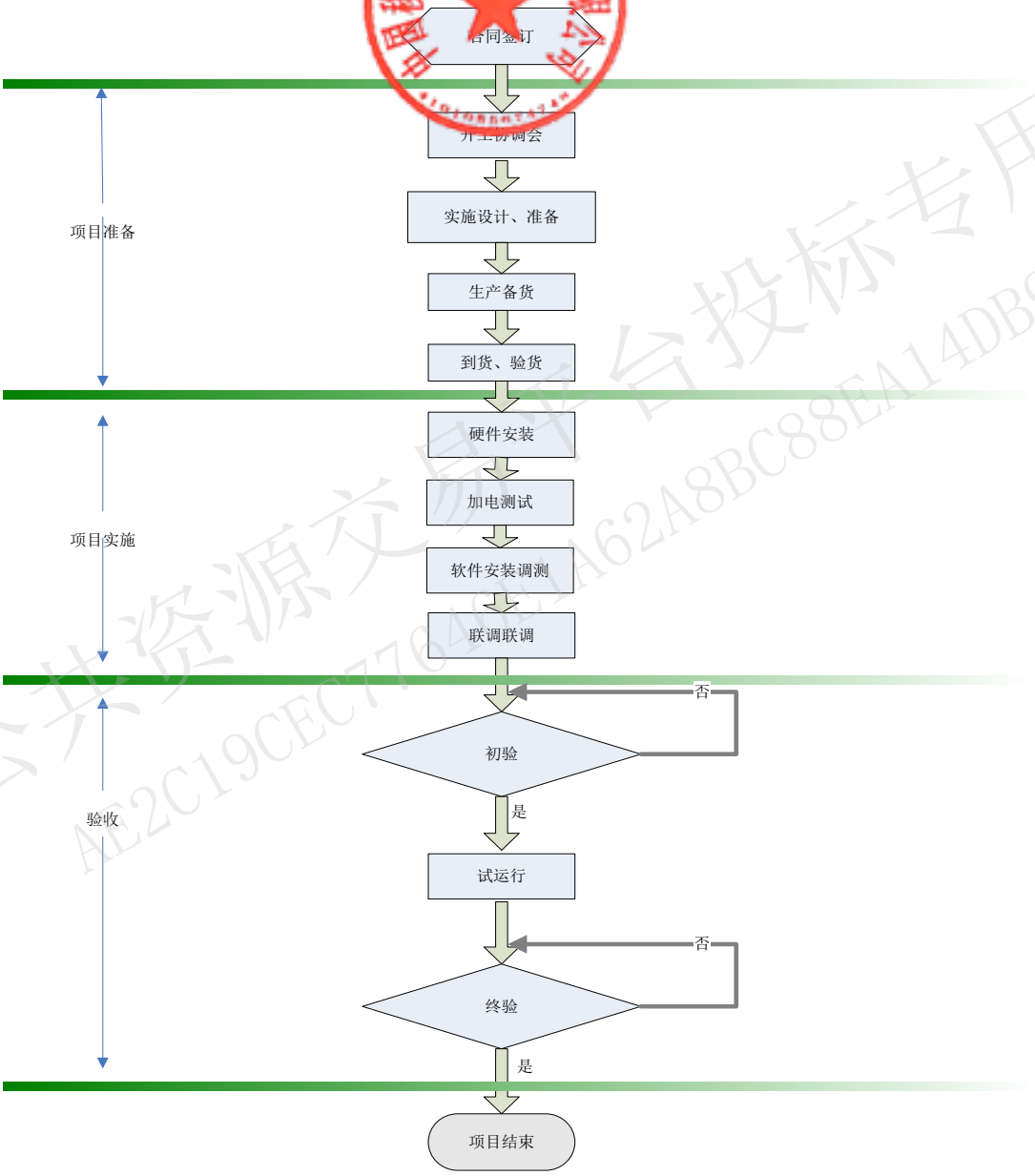
在问题与风险影响项目前对其进行处理

使时间与成本成为流程的入口

便于沟通、协调与合作

3.3.2.3 **项目实施的标准化流程**

从合同签署到项目终验需始终遵循下列流程：



公共资源交易平台投标专用
AE2C19CEC7764E1A62A8BC88EA14DB9

3.3.2.3.1 项目准备

（1）合同签订

合同签署后，我司将负责获得我司工程实施人员进入南阳市政府信息中心机房实施项目所需要的相关工作许可等。

（2）成立项目组

为保障项目的顺利实施，项目立项后，河南移动将成立高效的项目组织，组织结构包括项目管理、技术、质量、协调等职责。

在充分了解用户组织、合同信息、工程情况、货物、资源、条件的基础上，项目经理将与该项目共同商定制作工程策划报告，指导项目围绕质量、工期、成本、用户满意度高效益、高效率运作。

（3）工程技术协调会

河南移动将现场检验之前，在该项目制定地点举行一次工程技术协调会。工程技术协调会应包括但不限于以如下内容：

讨论交货的具体事宜。

该项目提供现场检验测试预案；河南移动提供现场检验的具体实施文件，河南移动提供与工程实际有关的技术资料以及与工程系统相关的图纸和资料，并由双方共同确认。

对供货合同清单中的项目和内容作进一步确认，并根据工程需要对供货合同清单中的项目和内容进行调整。

讨论解决合同实施中具体相关技术问题。

讨论确定本工程的各个系统及与周边系统对接的具体实施方案。

讨论河南移动提供的技术服务的具体实施方案。

施工进度及设备安装的安排。

双方认为需要讨论的其他问题。

河南移动将根据该项目的现网状况选择最佳的割接改造方案，为该项目提供最佳的服务和解决方案。

（4）勘测

河南移动根据合同约定或设备发货需求进行勘测。勘测期间，我司工程师将与客户合作执行详细的勘测，完成现场勘测和数据收集时，应由该项目与我司的项目代表签字确认“现场勘测报告”与“数据收集报告”。

（5）发货

公共资源交易平台投标专用

河南移动严格遵照合同要求，委托承运商分批/不分批将货物发运到合同指定地点。

我司在成交后按合同中规定的到货时间和地点完成所有设备的到货及设备检验/检测工作。

（6）环境准备

1）场地及机架准备

合同签订后设备到货前，由我司准备好位于河南移动数据中心的 IDC 机房，根据客户要求，划出独立的机房区域，等待设备到货。

2）网络环境的准备

网络物理连接图及设备上架安装位置；

确定 IP 地址规划和路由；

确定网络出口的申请；

交换机设备端口分配；

网络切换中可能遇到的问题和替代方案；

网络安全策略；

与政务外网专线的铺设等等。

3）场地检验

设备安装调试前，河南移动将联合客户及原厂商对机房条件进行检验，检验内容包括：

检验项目	检查内容（范例）
电源	机房是否配套的 UPS
	UPS 电源接地是否良好
	UPS 是否能提供交流 220V
	UPS 的最大负荷
	UPS 是否提供过载保护
	是否有备用供电系统
	是否配置相应的电源指示及检测设备
插座	机房相应的电源插座是否使用英式标准计算机通用插座
	是否提供设备主备电源的插座

公共资源交易平台投标专用
AE2C19CEC776E16E1A62A8BC88EA14DB9

检验项目	检查内容（范例）
机架环境	机架是否固定好
	机架是否通风良好
	机架固定是否符合抗震标准
	机房机架上是否提供良好的照明条件
	机房所有操作范围内照明条件是否满足
机架及工作站	是否安装相应数量的机架
	机架上空气开关的数量
	是否提供足够数量的计算机工作台
	机架上是否提供设备保护接地线
	接地保护线阻抗是否小于 2 欧姆
	是否有相应的配电屏
	相应架上设备所用信号线是否通过 PVC 管接至机架
线路	机房设置的走线槽方式（上走线槽或下走线槽）
	机房要求设置是否符合标准的架空上走线槽（使用上走线槽方式）
	使用下走线方式的是否采用 PVC 管安装电源线和信号线(使用下走线槽方式）
	电源与信号线是否分离
	各种线路是否标识明确
地板	防静电地板是否安装
	地板承重
	地板离地面高度
温湿	机房是否配有相应容量的空调系统
	机房温度是否保持在 20 摄氏度左右
	是否有相应的抽湿设备
	湿度是否低于 80%，同时大于 25%。
用具	是否配备常用工具
	是否配备常用线路

公共资源交易平台投标专用

检验项目	检查内容（范例）
	是否配备相关的测试仪表
防范	是否配有专用电话
	是否具备防火措施
	是否具备防雷措施
	是否具备防尘措施
	是否具备防静电措施
	是否有机房环境的详细布置图纸
	是否有机房环境的走线图
	设备安装时是否有熟悉机房环境的人员提供协助
	负责人名单和联系电话

（7）组织验货

到货时，河南移动提供的货物将在该项目业主代表和施工单位均在场的情况下进行开箱验货，合同产品的数量与外观将对照装箱单检查，我司有权派代表参加开箱验货。若由该项目业主代表与我司共同组织的检查发现缺货、损伤或与装箱单中列出的质量标准不一致，将由双方拟订一份详细报告并签字。检查要点为：

设备包装外观完好性检查；

拆箱后设备及板卡外观检查；

各箱设备及配件数量清点。

在上述情形中签字的检查报告将作为该项目用于要求我司换货、维修或补足的证据。若检查由该项目单独完成，并且未及时通知我司，则我司将不对检查结果负责，视同装箱单所列产品完整、完好的完成交接。

设备检验/检测通过后，由该项目和河南移动代表共同在装箱单上签字确认。

（8）现场校验

货物进场后，河南移动将与该项目在现场统一进行合同设备的现场检验，具体的时间安排将依据合同在工程技术协调会上确定的进行。

该项目将按照合同设备清单清点合同设备数量。

河南移动应在现场对合同设备完成单机加电、初始化及相关切换功能测试。

河南移动依照招标书中要求的网络部署图，将合同设备在现场搭建成实际运

公共资源交易平台投标专用

行环境，按照投标应答的技术规格，与招标人人员一起对系统的主要功能和性能进行现场测试，测试方案由河南移动将与该项目在合同签署时议定。

3.3.2.3.2 项目实施

（1）硬件安装

河南移动派出设备安装技术人员进行安装，设备安装的主要环节主要有：

方案制定

机架和子架安装

配线连接（配线主要包括机器正面、背面的各种电缆、插座及插片的连接）

电源线及地线布放

布放电缆和光纤

电路板的安装

其它部件的安装

系统上电开机

硬件检查

在整机调试前，必须确保各硬件检查准确无误，才能保证整机调试的顺利进行，硬件检查主要有以下内容：

各种插座无缺针、无内芯弯曲等现象，确保完好无损；

各种连线准确牢靠；

设备的各种选择开关应置于指定位置上；

各种插板插位准确牢靠；

设备标志应齐备正确；

设备内部的电源布线无短路现象。

（2）单机加电测试

检查确认机房电源环境，确认机房具备加电条件，对网络设备进行加电自检。观察并记录设备的启动过程、电源，风扇、主控和单板等运行状态。

（3）软件安装调测

设备硬件安装完成后，河南移动软调人员严格依照《数据设定规范》、《现场调测作业指导书》进行软件调测，并严格按照《工程文件》和相关产品的开局数据进行软件加载和调试。对《现场调测记录表》的每一项内容进行内部测试，并

公共资源交易平台投标专用

做好记录，为工程验收做好准备。 系统调试完毕后，对软件质量进行自检。

（4）联调测试

根据实施方案中要求，由该项目配合给出的各项业务参数,由河南移动工程师负责系统的的调测工作.主要包含如下方面内容：

1）在网络设备上配置认证管理参数,包括 Console、远程管理、AAA 认证以及 SNMP 等协议的配置；

2）联通性数据配置，包括接口的封装、IP 地址以及路由协议等。

在完成全部设备的系统调试工作后，我司 X 技术有限公司将在最终用户的协调下，完成与配套设备（包括本项目采购的其它设备、用户方其它项目近期采购的设备和原有设备）的联合调试，以构成整体的系统平台。

（5）现场培训

在工程实施期间，我司工程师根据实际需要可以安排对客户方项目工程师与技术人员进行现场培训，使该项目工程师掌握我司设备安装与调试的基本知识。

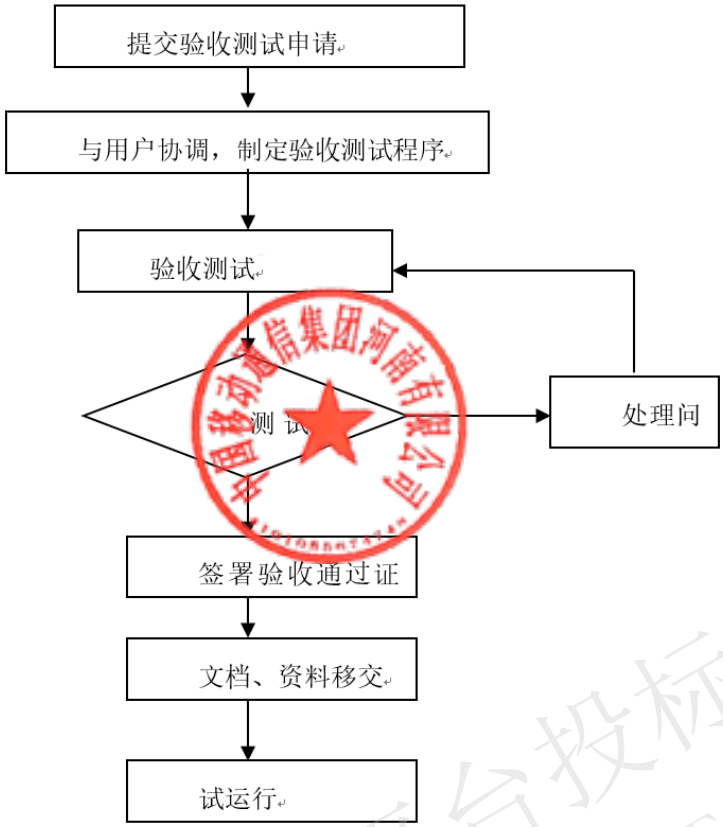
3.3.2.3.3 项目验收

（1）初验

初验是指进行设备移交时，由该项目与河南移动共同进行的系统测试。系统测试验收时，河南移动负责将测试项目明细表、测试方法、使用到的仪器、测得的各项技术指标值做好记录，输出验收测试报告。

测试验收流程如下：

公开资源交易平台投标专用
AE2C19CEC7FC1621A82A8BC88EA1



（2）试运行

在初验完成之日起在试运行期间内，期间由河南移动按正常维护规范要求进行例行测试，观察并做好维护记录和用户申告故障处理记录。对运行中的告警和各种软硬件故障应进行详细的记录和原因分析，对故障修复、更换坏件、修改软件程序等要有详细的记录。河南移动将及时向该项目提供技术指导，并适时派出经验丰富的技术人员对网络运行情况进行巡视和检查，以确保设备的正常工作。

（3）终验

在系统试运行正常结束后，整体系统进入正式运行的同时，应由最终用户方和我司技术有限公司等项目参与方共同对系统整体进行验收，整体验收的结果由参加整体验收的各方签名，形成整体系统验收报告（包括系统试运行期间有代表性的运行日志和记录），并且给出最终的明确结果：

通过整体验收；

未通过整体验收，延迟再作验收。

系统最终验收合格的条件必须至少满足以下三个要求：

已提供了合同的全部产品和资料；

试运行时间满足合同要求；

公开资源交易平台投标专用

性能测试和试运行时出现的问题已被解决。

整体系统验收程序如下：

1）验收前的准备：根据合同中的验收准则检查所有软硬件项及其整体系统配置是否完整，做好验收准备。

2）验收实施：根据合同要求或双方协商结果，确定验收时间、验收准则、软/硬件环境等，以及双方职责。

3）验收测试：测试项目应依照合同要求，可包括以下几项：

环境测试

可靠性测试

维护性测试

功能测试

稳定性测试

性能测试

4）编写验收报告：测试计划与测试报告格式及内容按照我司技术有限公司的相关规定及用户方要求执行。

5）问题处理：在验收（测试）过程中发现的问题根据合同规定来处理。如果合同中没有规定，应指明问题类型和责任归属，由双方协商解决办法。

系统终验合格后，由用户开具《设备最终验收合格单》。

设备最终验收合格单

文档编号			
合同名称		合同编号	
用户联系人		用户联系电话	
客户经理		项目经理	
参加验收人员		验收日期	
合同签订额			
合同验收内容			
1、设备开箱检验			

公共资源交易平台投标专用

2、设备加电验收	
3、产品初验测试	
4、系统初步验收	
5、系统最终验收	
我司 X 技术有限公司验收意见 签字：　　日期：　　我司 X 技术有限公司（盖章）	
用户方评价及验收结论： 1、满意　　2、不满意 评价： 1、同意验收　　2、不同意验收 结论： 验收方签字：　　日期：　　验收方（盖章）	

3.3.2.3.4　项目交付成果

我司项目组有专人负责项目文件的管理，所有项目文件（包括技术资料及工地现场文件）需交由该项目文档负责人签收，下表为交付件清单范例，实际交付清单可根据双方工程技术协调会一致的结论为准。

实施服务交付件清单（范例）：

序号	服务活动	交付件
1	项目管理	项目质量评估报告
		项目经验总结
2	需求调研	产品勘测报告、发货材料信息确认表
		客户需求项目确认表
3	硬件安装	安装环境检查备忘录
		客户签署的装箱单
		工程质量检测报告
		硬件安装竣工报告
		工程备忘录

公共资源交易平台投标专用

4	软件调试	软件版本、License 文件
		配置文件
		自检报告
5	系统联调	配置文件
6	初步验收测试	初步验收手册、签字表 系统上线报告
7	运行阶段	项目运行期维护手册
8	最终验收测试	最终验收手册、签字表 设备最终验收合格单
9	验收材料	主要包括服务能力验收、技术验收（性能、功能、信息安全等）、资料验收（主要包括建设方案、信息安全相关报告、政务云符合性测评报告、功能安全测试报告、系统安全性评估报告、机房图纸、运维方案等）。

3.3.2.4 **项目实施策略**

3.3.2.4.1 责任划分

安装服务实施责任界面

实施主体 工作内容	河南移动	招标方
一、工前准备		
1、安装环境准备	√	
2、工程安装规划	√	
3、确认安装条件满足要求	√	
二、软硬件安装		
1、开箱验货	√	
2、设备硬件安装	√	
3、设备硬件安装协助	√	
4、软件安装和系统调试	√	

公共资源交易平台技术专用
AE2C19CEC77646E1A62A8BC88EA14DB3

5、系统调试协助		√
三、测试及验收		
1、系统测试	√	√
2、现场培训	√	√
3、安装验收	√	√

3.3.2.4.2 实施计划

工期进度表的编制及实施计划的制定将根据以下原则制定。

1)可行性

工程进度计划将基于我们丰富的项目经验与对本地的深入了解制定的。 制定时间表的过程中，资源、时间、质量与成本因素均充分考虑。

2) 合理性

项目子任务与活动的关系符合我司现有流程，并考虑了客户需求与实际情况。

3) 效率

高效的工期进度表将使该项目与我司双方受益，并使该项目的投资收益最大化。

4）工期

签订合同后，5 日历天完成平台基本建设（含线路接入）。

3.3.3 质量保证措施

项目质量控制坚持“事前预防、事中控制、事后检查”的原则，重点落实“通过预防，不让问题发生”以及“防止发生过的问题再发生”，确保“按规范施工、按流程操作”，以“追求零缺陷”为目标，争取“一次性把事情做好”。

本项目将设置总体组质量经理，以客户满意度为中心，安装项目交付质量管理-“6 步 1 法”，确定质量标准、做好工前培训、示范站建设、质量自检和抽检、质量问题管理、质量总结。

公共资源交易平台投标专用



质量控制工作需要该项目客户与我司的共同努力。质量控制工作由我司质量保证系统监控，以确保产品和服务达到议定标准。我司的质量保证系统也将确保交付的产品达到业务要求，并持续改进质量控制流程。

3.3.3.1 **建立质量目标与方针**

（1）质量目标

保证各工程的施工质量，做到100%达到优良、100%按图施工、100%执行合同条款、100%做好竣工后的服务。

（2）质量方针

1）面向客户：质量的定义即符合要求，在开工前必须明确工作要求，要求来自内部上下游客户和外部客户。

2）面向业务：质量管理=业务管理，每个人都要对自己的工作质量负责，不接受上游的缺陷，自己不制造缺陷，不输出缺陷到下游。

3）预防为主：质量的核心是预防。通过流程和标准化杜绝问题的发生。事后检查只能发现缺陷，花费更大的成本整改返工。

4）持续改进：持续改进是组织和个人不断进步的根本。全员要树立持续改进的意识，不断识别业务中的改进机会并实施改进，促进组织和个人的能力和绩效不断提升。

（3）成立质量组织结构

在项目准备阶段，DQA（译文：数据质量评估）在整体项目组织结构的基础上可依据项目质量需求启动交付项目质量团队组建工作，制定项目质量团队组建方案，提交项目组讨论审批并发布；团队组建方案包括：项目质量组织结构、项目

公共资源交易平台投标专用

质量人员职责描述与活动、质量人员需求、质量人员获取方式。

3.3.3.2 **项目各阶段质量控制措施**

（1）项目准备质量控制

1）做好施工前准备工作，将组织优秀的工程技术人员和熟练的技术工人进入工程项目部，并进行专业技术培训。

2）对提供的合同文件和相关技术文件、报告进行详细审阅。能重点审核本改造项目的施工图纸是否完整、有无漏项、各文件之间有无矛盾、技术标准是否齐全、合同条件的细节等。

3）编制详尽的施工方案，并对施工图纸、施工组织设计进行交底，明确任务，分清责任。

4）对材料、工程设备的采购进行检查，检查采购是否符合合同的规定。对到场的材料及设备要及时检验。

5）准备好全部监理表格和质量管理表格，并对表格的作用和用法交底。

6）开好第一次工地会议，同业主和监理公司建立起良好的沟通网络。

7）操作人员严格按施工规范、工艺标准、作业指导书进行施工，做到持证上岗。

（2）施工阶段质量控制

1）工程督导在工地现场，不停巡视检查，及时发现问题，及时纠正、制止、预防质量事故于萌芽状态。

2）树立“质量就是生命”的思想，增强质量意识，高度重视质量工作，严作按照施工图、操作规程和质量检评标准组织施工。

3）加强岗位责任制，贯彻“谁施工、谁负责”，“谁操作、谁保证质量”的原则，严格实行工程质量与经济责任挂钩，严格按照我公司的奖罚措施执行，确保质量岗位责任制的实施。

4）严格进行技术交底，认真做好施工任务书的签发工作，各专业工长安排施工人员施工前必须要有书面的技术交底，其内容要包括：工作内容，施工工艺过程技术要求，质量要求，完成时间等，施工人员按照书面技术要求进行施工。

5）质量问题日清日结，当天回溯当天完成整改。

（3）检验阶段质量控制

公共资源交易平台投标专用

1）加强检测人员业务培训,对精密测试仪表操作经考核合格后持证上岗。

2）质检员根据检验控制程序对检验、试验进行监督，在检验和试验时要制定详细的检验和试验计划和方案。

3）隐蔽工程质量检验应同时具备自检合格记录与监理工程师的签认记录。

4）严格工程计量，从入库检查、施工测试到系统联调，按要求配置测试仪器仪表和操作人员,强化测试准确性,确保各项电气指标达到和高于国家、部标准。

5）加强对检验记录的控制、管理，使测试记录客观、真实、正确地反映工程施工实际情况，为检测结果的可追溯性提供详实的依据。

6）加强仪器仪表的日常管理和维护,确保投入本工程使用的仪器仪表精度和状态良好，按周检计划送检。

每个项目在操作过程中实行“三检”制。即操作者自检、互检，质量工程师专职检，保证各项目工序合格流转。对工程配备必要的检验、测量仪表，按要求完成各项目工程的检验、调试、测量与观测。我司在整个施工过程中，做好各种测试记录的收集、整理、保存。在工程完工后，将真实、准确的测试记录作为工程技术资料送交。

规范检验、测量设备的管理，以保证检验、测量设备的管理处于受控状态，测试人员上岗前，必须经过培训合格，确保测试数据的正确性。在施工中随时做到原始资料的积累、保管、整理，将真实、准确的各项测试记录，隐蔽工程记录、各项检验记录按合同要求送交，竣工资料、图纸做到清晰、明确、格式标准化。

3.3.3.3 现场质量检查制度

（1）开工前检查。检查是否具备开工条件，开工后能否连续正常施工，能否保证质量。

（2）工序交接检查。对于重要的工序或对工程质量有重大影响的工序，在自检、互检的基础上，还要组织本工程项目的专职管理人员进行工序交接检查。

（3）隐蔽工程检查。凡是隐蔽工程都必须在检查认证后方能掩盖。分项、分部工程完工，经检查认可，签署验收记录后，才允许进行下一步项目施工。

（4）设备保护检查。检查设备有无保护措施，或保护措施是否可靠。

3.3.3.4 项目例会制度

（1）运维团队采取周例会制度，例会人员包括云业务管理组、基础运维组、

系统优化组、网络安全组、机房运维组、云平台运维组的负责人和经信委运维经理；

（2）各小组在会议上向经信委运维经理汇报上周的重大运维事件，安排下周的运维计划；

（3）会议后由云业务管理组输出会议纪要存档。

会议纪要模板：

会议名称	XXX云例会
会议时间	XXXX年XX月XX日（星期X）上/下午
会议地点	
参加人员	XXX相关人员 云业务管理组： 基础运维组： 云平台运维组： 系统优化组： 云平台安全组： 机房运维组： 专家支撑组：
会议结果	
一、 重大运维事件/故障分析 二、 总体运行情况汇报 三、 下周重点工作安排 四、 需协调问题	
XXXX年XX月XX日	
联系人：	

3.3.3.5 **沟通计划及汇报机制**

项目沟通管理包括项目运作过程中及时有效地制作、收集、传播、存储并最终处理的项目信息，主要过程包括：

沟通计划：确定客户项目组成员的信息和沟通需求，即明确项目信息的提供

公共资源交易平台投标专用

范围、时机、和沟通对象。

信息传播：保证所需的信息及时有效的到达项目组成员和其他利益攸关的各方。

绩效报告：收集和传播性能信息。其中包括状态报告，进度测量和预测。

管理闭环：产生，收集和传播信息至项目正式完成阶段。

上述流程将贯穿项目实施的整个过程。

周报汇报方式：每周由云业务管理组牵头，组织云平台运维组编写周报总结输出；

月报汇报方式：在内部组织内审核通过确定月报内容完全正确后，跟客户汇报月度报告。

3.3.4 风险管理措施

通过持续关注风险管理，项目组将把潜在的负面事件及其对项目的影响降至最低，以便提高项目成功的可能性。

风险管理主要包括：

3.3.4.1 项目风险管理目标

本项目可能存在的风险及拟采取的相应措施主要包括以下几个方面：

风险分析是项目管理方法论的一个最重要环节，是在项目实施的全过程中始终关注对于风险的管理。本阶段的主要风险集中在如何有效的确定和把握用户需求，并在建设内容上平衡好基础应用建设和业务应用建设之间的关系。下面是针对本阶段项目的风险管理建议。

（1）准确把握需求

在项目初期对整个项目进行工作分解，分解成一个个的子项目。并在每个项目开始后，首先与建设单位一起对该项目的功能需求进行详尽的需求分析和技术设计，并形成分析和设计文档。在广泛听取其他部门和相关领域专家的意见后，确定项目的最终需求。

（2）管理好项目的进程

本阶段项目中的第二个风险因素，是对于项目进程的管理。其中一个关键措施，是建立一个有效的项目管理机构。建议共同成立一个项目管理委员会，每周开会检查项目进度，随时协调解决项目实施中出现的问题，以保证项目的顺利进

公共资源交易平台投标专用

行。

（3）从建设内容上减少项目风险

系统平台是支撑各类应用的运行环境，要考虑支撑能力、可扩展性、先进性和开放性等因素，主要包括操作系统、目录服务、数据库管理系统等。分步实施，先实施信息化基础好，条件成熟的子系统，在此基础上，建设复杂的系统，最后是关联性最强的共用相关模块。最常用的、基础的应用建设，依次规避建设风险。

3.3.4.2 项目风险管理流程

对整个项目实施周期及风险要有把控能力，能够提前梳理出项目实施难点及风险点并制定详细的解决措施。

（1）项目风险管理

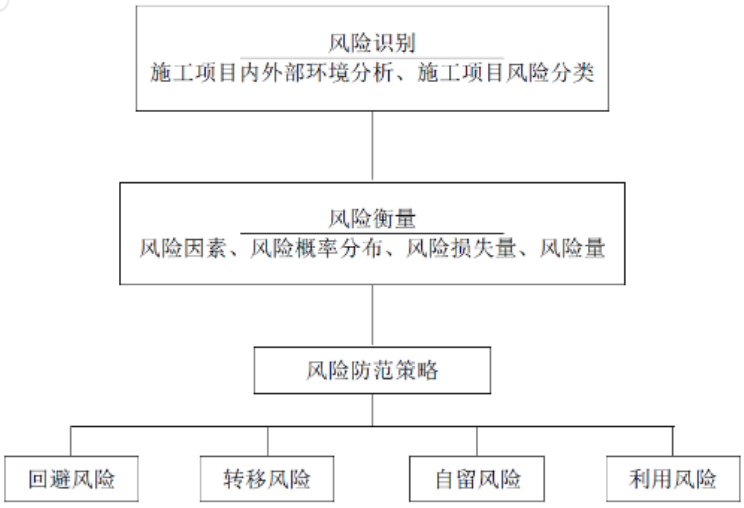
风险管理是对风险的不确定性及可能性等因素进行考察、预测、分析的基础商，制定处包括识别衡量风险。管理处置风险、控制防范风险等一整套科学的管理方法，对项目管理工程中的每个阶段所包含的全部风险通过识别、衡量、控制，使工程顺利进行，减少风险损失，创造更大的经济效益。

（2）项目风险管理目标

根据现阶段我公司的整体实力，制定如下风险管理目标：“降低风险管理成本、提高利润，树立信誉、扩大影响，拓宽业务渠道”。

（3）项目风险管理流程

项目风险管理流程一般分为风险识别、风险衡量、风险处理与风险防范对策四个阶段，各阶段及其内容如下图：



（4）风险的分析及评估

公共资源交易平台投标专用

根据风险存在的来源，性质，出现的频数，危害程度进行分析和评估，确认其可能产生，并做到事先预防，事中处理，事后有应对措施。本工程项目风险存在的可能性划分，项目风险主要有以下几个方面：

技术风险、管理风险、过程控制风险、质量风险、职业安全风险、市场风险、法律法规、环境风险、业主及利益相关者。

（5）风险的应对措施和等级

风险等级划分见下表：

序号	风险种类	风险内容	影响结果	危害程度	应对措施		
					事前	事中	事后
1	技术风险	施工方法选择不当	影响质量与进度	高	多技术方案比较、优化	制定补救措施	评估事件，技术改进
2	管理风险	管理不到位； 个人能力、施工队素质；	质量不达标 进度不达标 安全不达标	高	明确管理机制； 施工预审	调整组织结构； 启动备选施工队	评估事件原因； 将施工队从剃出合作
3	过程控制风险	协调不到位	工程质量和进度不达标	中	工程例会协调	强化施工过程管理	进行总结，管理改进
4	质量风险	质量缺陷	达不到预期合同质量等级要求	中	制定创优计划	分析质量原因，调整管理方案	质量总结 开质量分析会
5	职业安全风险	安全事故传染病	工期延误	低	制定应急预案	启用应急预案	调整应急预案

公共资源交易平台招标专用

			费用增加			进行总结	
6	法律法规	时间限制路段限制政治需要	工期影响	低	与周边做好信息沟通	调整施工作业时间	制定补充计划
7	环境风险	环保不达标	停工	低	制定环境管理计划，制定预案并检查	及时整改	对责任人处理

3.4 一体化运维服务方案

我方提供素质高、专业性强、经验丰富、稳定的运维团队，主要负责整个政务云平台的软硬件和网络运维。我方能为本项目选派专业技术人员参与本项目实施运维，运维人员 14 名，包括云核心技术提供方的原厂或原厂授权运维人员 6 名、其他运维人员 8 名。投标人需有严格的、有组织、有纪律的管理运维流程，并指派专职联络员，团队需要 7×24 小时在岗及时响应故障请求，负责云平台的故障受理、处理、跟踪、结果汇报工作。

为保证云平台服务可用性及运行效率，供应商云平台的服务能力须保证各个应用系统可用性不低于 99.99%；供应商云资源交付响应时间不超过 2 个工作日。

运维方案应从整运维服务体系的宗旨、运维服务体系架构、运维服务体系的内容、运维管理制度、人员培训等方面来阐述说明。

3.4.1 运维服务体系的宗旨

我方具有完善的服务保障体系（配备有足够的、有相应资质的专业技术人员），并对所租用的货物的品质和服务负责。

我方将积极配合采购人进行政务应用系统部署、调测、试运行、升级等一系列内容，在政务云机房提供 7*24 小时的配合服务。

我方自行解决产品的硬件升级、现场保修、技术支持、运维服务等。

我方保证所提供硬件产品包括相关附件为相应硬件厂家原装正品，软件产品为相关厂家正版软件，符合国家有关规定。我方保证所提供产品具有合法的版权

公共资源交易平台 技标专用

或使用权，本项目提供的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，由我方负责，采购人不承担责任。

我方提供的服务不得低于标准服务，即与投标产品制造厂商通过网站等对外公布的有效服务标准相一致。在标准服务基础上，我方承诺达到以下标准：

产品是符合国家技术规范和质量标准的合格产品，满足采购单位的使用需求，并具有可靠的售后服务体系，质量可靠、使用安全。

保证提供的产品中所有预装和为本项目安装的软件均为具有合法版权或使用权的正版软件且无质量瑕疵；

保证所供货设备必须是厂商原装的、全新的、性能完好的，型号、性能及指标符合国家现行的及竞争性磋商文件提出的有关技术、质量、安全标准。

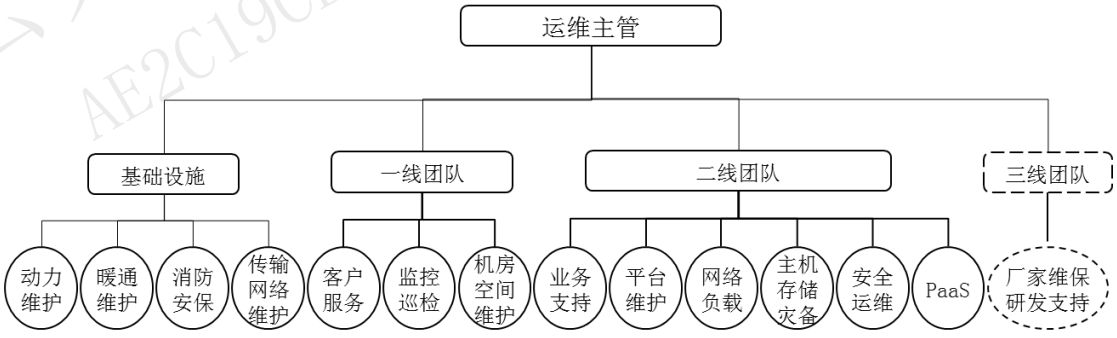
所有设备数量、质量及性能不低于本文件提出的要求且集中管理。

我方运维团队将安排云平台、云安全原厂技术人员提供南阳本地运维服务，制定并遵循运维管理制度与服务流程，提供 7*24 小时政务云数据中心现场支持服务。

3.4.2 运维服务体系架构

3.4.2.1 组织架构

我方配置专职的运行维护和技术支持本地团队，具备云计算、网络、存储、数据库维护能力，提供 7*24 小时机房现场关键角色值守服务，设置统一服务电话，及时响应服务请求及平台故障，支撑云平台日常和网络的运行维护工作。



南阳移动运维值班电话：0377-83889600

运维团队配置原则：

1、根据政务云涉及模块分别配置人员

2、同一岗位设置 AB 角色，互为备份

公共资源交易平台投标专用
AE2C19CE6776161A62A8BC88EA1

3、关键岗位（云平台、云安全）配置原厂人员支撑

4、本地化 7*24 小时值守

根据本项目要求支撑人员如下：

序号	姓名	公司	专业分工	资质水平
1	谌伟超	中国移动通信集团河南有限公司	数据中心机房运维 A	高级工程师
2	高阳	中国移动通信集团河南有限公司	数据中心机房运维 B	高级工程师
3	郭晓玲	中国移动通信集团河南有限公司	动环设施运维管理 A	高级工程师
4	黄伟	中国移动通信集团河南有限公司	动环设施运维管理 B	高级工程师
5	李军	中国移动通信集团河南有限公司	监控、消防、安保管理 A	高级工程师
6	郝文胜	中国移动通信集团河南有限公司	监控、消防、安保管理 B	高级工程师
7	蒋纬昌	中国移动通信集团河南有限公司南阳分公司	运维服务 A	网络工程师、网络安全
8	高锋杰	中国移动通信集团河南有限公司南阳分公司	运维服务 B	云应用集成交付工程师
9	姚鹏	华为云计算技术有限公司南京分公司	云平台维护 A	云服务解决方案架构师
10	王春光	北京华为云计算技术有限公司	云平台维护 B	云服务解决方案架构师
11	胡辉	华为技术有限公司北京研究所	云平台维护 A	云服务解决方案架构师

公共资源交易平台投标专用

12	冯纯硕	华为安驰智行技术有限公司	云平台维护 B	云服务解决方案架构师
13	李东伟	西安华为技术有限公司	云安全维护 A	云服务解决方案架构师
14	张哲千	华为技术有限公司	云安全维护 B	云服务解决方案架构师

3.4.2.2 运维范围

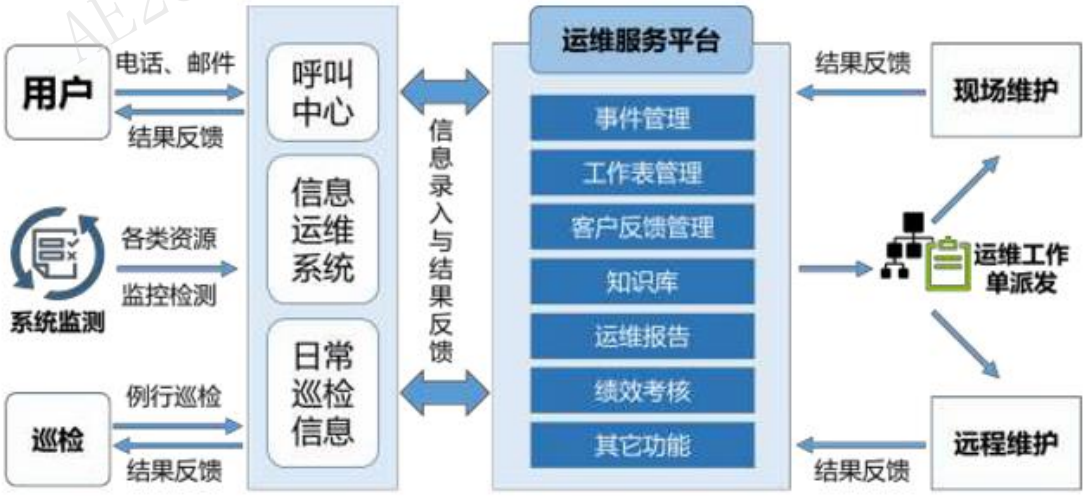
针对南阳政务云平台涉及的公有云与专有云运营维护，配备专业的维护团队，提供全面的保障及运维服务，运维管理对象包括：机房、网络设备、安全设备、虚拟机、物理机、存储。集中专家资源解决运营维护过程中的各种疑难故障和问题，提升故障响应速度和本地业务支撑力度，确保南阳政务云平台高效、稳定、持续提供高可靠性的云服务。

3.4.2.3 工作流程

我司基于一整套完善的运行保障体系，组建云计算专业团队，为南阳市政务云平台项目云提供 7*24 小时运行维护服务。

运行保障服务可概括为“两个一”，即制定一套完善的运行保障流程制度、组建一支专业的运维服务团队，基于此开展运维管控及持续改进。

项目运行保障服务总体示意图如下：



（1）制定一套完善的运行保障流程制度

1）制订完善运行保障服务流程；

2）制订完善运行保障管理制度；

3）制订完善日常运行保障服务规范；

4）制订完善各项预防和应急保障制度；

5）制定完善各项指标体系。

（2）组建一支专业的运行保障服务团队

1）运行保障管理组织机构的建立；

2）运行保障服务人员定岗定责；

3）运行保障服务人员技能、业务培训。

（3）运行保障管控及持续改进，通过分析改进提高运行保障管理质量

1）服务事件跟踪、反馈和回访；

2）运行保障服务流程监控；

3）服务质量监控；

4）运行保障管理体系运行监控；

5）服务流程的改进和完善；

6）服务质量的完善和修订。

3.4.2.4 **服务年限**

针对南阳政务云平台，提供 3 年 7×24 运维服务。

3.4.3 运维管理制度

3.4.3.1 运维管理

3.4.3.1.1 机房环境管理制度

河南南阳移动为政府各厅局提供高质量云服务，设置机房维护组负责做好电力、空调、消防、安全等机房环境设施的保障工作:

机房运行环境的管理

河南南阳移动为政务云数据中心机房环境及配套的基础设施提供专门的运维保障，提供高质量、安全可靠的运维服务，达到运营管理中的可靠性目标。

基础设施及现场机房环境维护

机房现场日常维护时间：7*24 小时。机房所提供的基础设施维护内容包括：

公共资源交易平台投标专用

对政务云机房专有的配电系统、空调系统、消防系统、漏水检测系统及安防系统的日常巡检及保养维护。

建立积极有效的监控管理机制，通过场地与环境集中监控系统对相关设备系统进行监控和记录，及时处理发现的故障和隐患，以保障所提供的政务云机房的基础设施和机房环境的稳定与正常。

供配电系统维护

机房维护人员负责政务云机房所配备的冗余变压器、高压及低压配电系统、后备柴油发电机、UPS、开关电源等设备的日常巡检与维护，定期巡检、记录机房配电系统的运行情况，发现问题及时处理。

空调系统

定时检查机房的环境温湿度，确保政务云机房始终处于在 23℃±2℃间、湿度在 55%±15%之间的恒湿、恒温状态。

定期记录空调系统运行情况，发现问题及时处理。

消防系统

委托具有消防设施维护保养一级资质的专业消防维保企业对机房楼的火灾报警系统、气体灭火系统、消防广播系统、防排烟系统等消防系统进行日常巡检维护和检测维修，确保消防设施正常运行。严格按照行业规范对气体灭火钢瓶定期进行检测，对机房内电（光）缆管道、竖井、孔洞进行防火封堵。

每个独立区域内均建有微型消防站，组建义务消防队，要求每季度至少进行一次消防培训和演练。

机房灭火应急预案

1、 机房一旦发生火情时，应及时切断着火设备及着火区域电源，积极组织现场人员进行扑救，同时立即上报主管领导。

2、 在火势初起阶段，应充分利用配备的消防器材，将火势控制在最小范围内并将其尽快扑灭。

3、 因火势蔓延，用一般灭火器不能将火扑灭时，通知消防中心监控室，并说明政务云机房发生火灾所在的消防区域，消防中心应立即启动手动或自动相应消防区域的灭火装置，进行扑救。

4、 在无力自灭自救时，一方面组织义务消防队积极抢救、疏散人员和物资

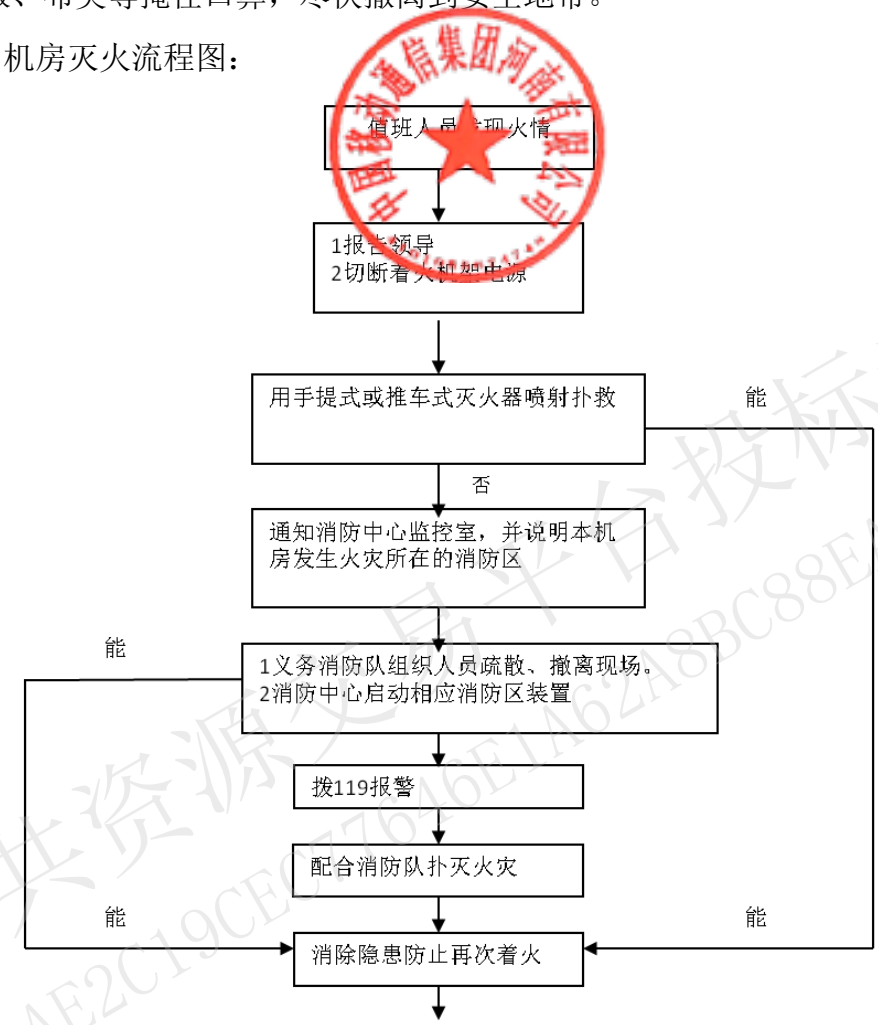
公共资源交易平台投标专用

设备，另一方面，要迅速拨打“119”报警。

5、 消防队赶到后，要安排专人尽快向消防队介绍火场情况，及时讲明起火部位，内部基本情况等，并积极协助其进行灭火工作。

6、 疏散人员时，为了防止烟雾中毒、烧伤等意外的发生，应用湿毛巾、湿衣服、布类等掩住口鼻，尽快撤离到安全地带。

机房灭火流程图：



消防管理制度

1、 广泛深入地进行防火宣传教育，贯彻执行“预防为主，防消结合”的方针，发动群众杜绝各种火灾事故的发生。

2、 凡有火源的地方都要做到火源附近不准堆放易燃易爆物品，动用明火需报经保卫部门批准并有动用明火的通知。

3、 易燃易爆物品要妥善保管，并由保卫部门监督。

4、 电器设备的安装、修理由正式电工负责，如需使用各种电器应先报请网

公共资源交易平台投标专用
AE2C19CE...

络部安全管理员批准，且不能超负荷使用，发现不安全因素时，立即停止使用该用电器，断电后及时报告有关领导。

5、 机房、仓库、油库、汽车库等不准使用各种明暗火，严禁吸烟，严禁存放易燃易爆物品。

6、 配备的灭火器应有专人保管，放在使用方便的位置上，定期进行检查，维修，按时换药。

7、 机房维护人员应加强防火安全学习，定期检查相关防火设施，开展防火救火演练，每季度要进行一次全面的安全防火检查：必须确保有关环境监视告警装置的可靠性。

8、 确保机楼消防设施完好，机房内必须按规定配备消防器材及防毒面具，并放在明显便于取用的地方：必须装设烟雾报警器，由专人负责定期检查。每个维护人员必须熟悉基本的消防知识、会用消防器材。

机房安全生产制度

1、 机房维护人员要认真学习，严格遵守政务云机房安全生产制度，严格遵守用电、防火的规定，作好防火、防盗、防爆、防雷、防潮等工作，确保人身和机房设备安全。

2、 机房内非特殊要求，严禁使用明火。若确实需要，需经相关部门批准，并采取相应严密措施后，方可动用明火。

3、 各种通信线、直流电源线、交流电源线应分别布放：电源线路和设备的安装要符合相关规范要求。

4、 机房内禁止吸烟，禁止将食品带入机房：严禁存放和使用易燃易爆及腐蚀性物品、机房内的电缆井、穿墙孔洞要用阻燃材料封堵。

5、 机房内未经维护部门批准禁止私接电源线、机房禁止安装、使用高温照明灯具、电炉、电热水器等电热器具。

6、 机房应安装可靠的避雷装置，各种防雷设施性能完好并可靠接地，雷雨季节要加强对机房内安保设备、地线及防护电路的检查。

7、 各类机房均需配备相应的消防器材，并安装有效的烟雾、高温、防盗告警设备。

8、 在机房内登高作业时，必须使用绝缘梯凳，不得在机柜内、机柜顶和走

公共资源交易平台投标专用

线架上放工具、工具袋及其它物品，以防工具等散落损坏设备和伤人。

9、 机房门内外，通道、路口、设备前后和窗口附近，均不得堆放物品和杂物，要做到无杂物、无垃圾、无污水，以免妨碍通行和工作。

3.4.3.1.2 机房值班制度

1、服从指挥，安心本职工作，实事求是地完成机房巡查、设备周期性维护作业等基础维护工作，确保设备和网络处于安全运行状态。严格执行各种操作流程。

2、准确、迅速地处理障碍和告警，并做好相应记录；遇重大障碍要及时向上级主管领导及相关部门汇报；不得以任何理由推诿、拖延处理障碍时间。

3、不得随意关闭设备告警，不得人为切断和私人占用电话，保证机房测试和值班电话正常，所有个人通信工具必须 24 小时正常开机。

4、遵守故障和投诉的相关处理规定，准确迅速地处理申告和故障，及时查询、传报、汇报和核对，不得以任何理由和借口推诿、拖延处理时间。

5、及时、准确、完整、如实地填写值班日志和各种指定填写的记录。

6、严格遵守通信纪律和安全保密规定，遵守机房管理制度，遵守机房作业管理规定。

7、当有两人以上同时值班时，应指定一人负责值班期间的全面工作，未经上岗考核或不合格的人员，不得单独承担值班工作或独立操作。

3.4.3.1.3 机房安全管理

为确保政务云机房的安全可靠，建立有效的安全机制，机房场地的安全制定了安全管理措施：

现场值班人员通过门禁系统控制对政务云机房的访问，非授权人员不得进入。

政务云机房配备全球眼监控系统、对机房实行 7*24 小时的实时监控。

对机房内所有物品实行严格的事前进出审批及进出登记制度，对记录文档妥善保留一年。

对授权进入机房内的服务厂商，全程陪同并作记录。

3.4.3.1.4 机房人员管理制度

1、 值班人员实行 24 小时值班制度，值班期间严禁串岗、溜班，严格遵守值班制度，未经批准不得擅离职守和调换班次。

公共资源交易平台技术专用

2、 保持机房整洁，物品摆放有序，工作台上严禁放杂物。

3、 严格执行各项有关设备维护规程，按时制定完成个人维护作业计划，填写工作记录。

4、 严格执行各种操作规程，遵守人机命令管理规定。

5、 当发生故障时，要立即通知相关部门并积极配合，及时查询故障排除情况，做好详细记录。

6、 值班人员是故障第一发现人，若有重大故障发生，要迅速报告主管领导，并做好现场预处理工作，记录故障产生时间，现阶段处理情况，及时做到各职能部门信息的沟通工作。

7、 严格执行出入登记、监督配合外来人员工作，防止和杜绝因操作不当影响云服务质量或人为障碍。

8、 爱护公共物品，正确使用工具仪表及技术资料监督执行微机系统管理制度。

9、 政务云机房要本着保证全程全网云服务稳定为宗旨，主动配合处理业务故障。

维护人员岗位责任制

1、 严格遵守各项规章制度和操作规程。

2、 熟悉维护设备、链路的性能原理，具备对本系统进行监控、正确检查运行情况的能力。

3、 认真执行作业维护计划，负责设备的维护和检修、云平台健康巡检。

4、 及时处理设备的工作，如有未解决故障和故障隐患及其他疑难问题，及时和有关人员联系，尽快解决。

5、 按上级管理部门要求，执行局数据修改，配合软件更新操作。

6、 参加运维项目组管理，质量分析活动。

机房出入登记制度

1、 进出政务云机房的登记人员应包括：除本机房维护人员以外的所有外来人员。

2、 外来人员不得擅自进入机房，如需进入，需经有关部门批准，并进行登记后由机房维护人员陪同方可进入。

公共资源交易平台技标专用

3、 所有进出机房的外来人员及其携带的物品，均须接受机房维护人员的检查，并如实填写机房出入登记表，经机房维护人员确认无误后方可进入。

4、 外来施工人员除需填写机房出入登记表外，还需出示机房施工进出审批表及本人有效身份证件，经网络部批准后才能进入机房施工。

5、 外来人员进入机房，需遵守机房相关管理规定，保持机房卫生、整洁，进入机房必须换机房专用鞋或戴鞋套。

6、 外来人员进入机房必须遵守机房相关管理规定，非经机房主管同意，不得随意碰触设备及终端，也不得翻阅图纸及其他相关资料。

7、 以上对政务云机房出入登记的相关管理制度解释权归南阳移动公司网络部，对于不服从以上机房出入管理制度的外来人员，机房维护人员将有权拒绝其进入机房。

机房操作管理制度

1、政务云机房的数据实行双人作业制度；操作人员遵守值班制度，不得擅自脱岗。

2、值班系统管理员必须认真、如实、详细填写《系统管理员机房操作日志》等各种登记簿，以备后查。

3、 严格按照每日预制操作流程进行操作，对新上业务及特殊情况需要变更流程的应事先进行详细安排并书面报负责人批准签字后方可执行；所有操作变更必须有存档记录。

4、 每日对机房环境进行清洁，以保持机房整洁；每周进行一次大清扫，对机器设备吸尘清洁。

5、 值班人员必须密切监视中心设备运行状况以及各网点运行情况，确保安全、高效运行。

6、 严格按规章制度要求做好各种数据、文件的备份工作。中心服务器数据库要定期进行双备份，并严格实行异地存放、专人保管。所有重要文档定期整理装订，专人保管，以备后查。

机房安全保卫

1、 机房工作人员，要有较高的思想素质，熟悉机房的基本情况、规章制度和保卫措施，忠于职守，尽职尽责，严守机密。

公共资源交易平台投标专用

2、 要害部门的安全保卫工作，必须坚持“谁主管，谁负责“的原则。

3、 机房必须控制闲杂人员进入，不准存放任何易燃易爆物品，严格执行机房出入登记制度。

4、 对机房要经常进行安全检查，及时整改安全隐患，做到防患于未然，确保机房的安全。

5、 单位领导要经常对机房工作人员进行思想和保密教育，增强政治责任心，确保机房万无一失。

3.4.3.1.5 安全保密制度

1、 严格遵守保密纪律，增强法制观念和保密观念，不随意监测用户数据，不得随意增删，泄露有关资料。

2、 机房工作人员在处理业务流程过程中，接触到的数据等必须严守秘密，不准向任何人泄露，更不准擅自将用户资料带出机房。

3、 严格管理机房内各种涉及机密的图纸、资料、文件等，并认真履行使用登记手续，不准携带机密文件进入公共场所或探亲访友。在私人通信、广告宣传中，都不得泄露通信机密。

4、 非业务部门人员或外来人员因公进入机房时，须经有关部门批准，并进行登记后方可进入。进入机房必须遵守机房管理规定和机房安全规定。

5、 机房工作人员在处理完业务时，应当随时整理相关资料并存档或转送有关部门，不得散放于桌面，任人翻阅。

6、 机房人员在受理司法部门查询时，必须有相关领导和专职安全员的签字手续，并进行存档登记。

7、 机房人员不准在公共场所谈论机房数据，机器设备性能，不准泄露用户资料。

8、 所有维护和管理人员，均应熟悉并严格执行安全保密规则。

3.4.3.1.6 安全应急预案

为了保障政务云机房和综合楼生产用电安全，一旦电源出现故障，能及时处理和尽快恢复正常供电，特制定本预案。

应急预案启动条件:

本预案适用于政务云机房生产电力保障，在突然出现局部停电或高压供电设

公共资源交易平台技术专用

备发生故障时，可立即启动本预案。

应急预案执行原则:

当出现局部停电或供电设备故障时，单位配备的发电机组立即启动进行供电，首先保证政务云机房用电，保证政务云生产机房用电安全，确保政务云服务与厅局业务正常运行。

预案保障措施:

1、 按照工作计划对电源设备、蓄电池、UPS 等配套电源设备进行检查和维护，排除存在的故障隐患，始终保持电机、蓄电池容量正常和完好。

2、 坚持保养维护制度，开展日常演练，熟悉油机启动和停送电的模拟供电，保证每个人都能掌握油机启动步骤和停送电步骤。

3、 按照规定每月对发电机组进行开机试运行，确保油机在紧急情况下 10 分钟内可以正常启动进行供电。

4、 与电力部门保持联系，了解市电停电情况，确认停电性质和估测停、来电时间，及时对油机燃料等进行相应调整。

5、 电力值班人员对重点部位增加巡检次数，确定每个设备厂家的售后维修联系方式，出现不能解决的故障及时与厂家技术人员联系，寻求支持。

3.4.3.2 **管理流程**

为了保障南阳政务云平台的云服务质量，基于 ITIL 运维管理最佳实践，在本项目中定义的运维管理流程包括：事件/故障管理流程、变更管理流程、资源管理流程、监控与告警管理流程、备份与恢复管理流程和运维报告管理，将政务云日常运维活动科学化、标准化、流程化。

3.4.3.2.1 事件/故障管理

流程目的

事件管理流程的主要目的是尽快解决运维中出现的事件与故障，尽快恢复业务，保障运维服务达到服务水平协议。

通过对事件进行登记、分类、分级、状态跟踪、关闭确认等手段建立一个事件管理流程的闭环，从而对事件的处理过程进行监控和优化。

定期对事件信息进行统计和分析，了解事件与服务请求的分布和发展趋势，降低事件响应时间和解决时间。

公共资源交易平台投标专用

流程原则

1） **管理原则**

所有南阳移动政务云维护范围内发生的事件，都应该记录管理，记录的信息应足够详细，包括事件处理交互过程，详细的解决方案。

所有支持人员对优先级为紧急和高的事件所采取的服务恢复行动，在比对其它行动的时候，将拥有优先处理级别。

2） **责任人原则**

所有权原则用来确保每个事件在任何时段都有适当的人员负责。由各厅局用户申报的事件单，服务台是该事件的责任人，必须确保事件得到有效跟踪与解决，并负责事件单的关闭。当事件单被分派后，接单的事件处理员作为此事件当前责任人，负责对事件进行处理。

3） **关闭原则**

由用户申报的事件单，关闭必须由服务台完成。事件处理人员在解决完成事件时，根据实际解决情况填写事件的解决方案，服务台负责和用户再次确认事件是否解决。

4） **优先级原则**

事件的优先级表明了该事件对用户的业务影响和紧急程度。它是评定事件或服务请求处理优先顺序、解决时限的一个重要指标，优先级决定处理事件的顺序及所需的资源。

5） **目标解决时间原则**

为了更好地控制事件的解决过程，事件管理流程被分解成几个阶段。每个阶段都设定相应目标时间。

6） **升级原则**

事件的升级方式为技术升级和管理升级。技术升级是基于时限要求或技术能力要求而将事件受理转移给更高级别支持小组的操作。例如，一线转二线。管理升级是指在当前层级无法处理事件时，需要通知管理层，利于资源的投入。

3.4.3.2.2 变更管理

流程目的

变更管理主要目的是规范云平台生产环境变更活动，确保所有变更行为能准

公共资源交易平台投标专用

时完成，并且不会导致服务意外中断，降低风险，保证云平台生产环境的稳定性、可靠性、安全性，并最大化地提升云平台的可用性。

流程原则

1） 管理原则

所有涉及运行环境的变更都必须严格遵循变更管理流程；所有变更过程信息都应被记录并可追踪。

2） 审批原则

在变更管理流程中应充分考虑“风险”和“效率”的平衡，通过对变更的充分评估和审核控制变更的风险，但对不同类型的变更在流程或审批路径上区别对待，以达到高效的目标。

3） 变更窗口原则

变更窗口原则用于确定变更实施的日程。变更窗口通常选择云平台运行对业务影响最小的时间周期，在规定的变更冻结期内，原则上禁止变更。变更窗口机制应当形成书面文件并公布，供所有参与变更人员使用。

4） 前导时间原则

前导时间是指从提交变更到变更实施之前所需要进行评估、审核等准备活动的最少时间。前导时间是基于变更影响度而定的。实施变更需要适当的前导时间进行评估和制定计划。

5） 回退原则

当变更实施失败或者无法在规定的时间内完成，则需要进行回退。任何回退的变更将作为变更失败而关闭，在下一次实施前，变更请求者必须重新提交新的变更请求单(RFC)，以便重新进行审批。

6） 关闭原则

变更实施完毕并且得到确认后，将由变更申请人关闭请求单。变更之后如果引发了其他问题，将更新变更单的信息。

3.4.3.2.3 资源配置管理

流程目的

通过识别、控制、维护、核对、汇总南阳政务云基础架构的各资源要素的配置信息，为 IT 基础架构或某个具体服务的搭建起一个逻辑模型，实现信息的公

公共资源交易平台投标专用

开与共享，使南阳政务云平台能为各厅局租户提供的服务在一个合理的性价比范围以内。并为其他管理流程（变更、发布、事件、问题等）提供一个基础支持，如变更流程中风险控制需要准确的配置信息作为判断依据。

流程原则

1） 管理原则

资源管理流程通过对云计算、存储、网络、安全等资源与服务的调配进行申请、审批、登记、部署、状态跟踪和关闭确认等活动建立了一个管理闭环，从而确保资源合理分配和使用；同时，定期对资源使用情况进行统计和分析，了解资源的分布和增长趋势，为 IT 基础设施资源池的容量管理和业务产品 IT 基础设施成本投入决策提供数据支撑。具体管理原则如下：

a） 资源管理流程是对云服务资源占用的唯一入口；

b） 完整、准确地记录所有资源申请、审批、部署、使用、调整、回收等过程，以确保资源使用信息与物理环境一致；

c） 定期生成各业务资源使用情况和 IT 资源池容量管理报表；

d） 定期对资源管理流程进行回顾和优化改进。

2） 责任人原则

资源管理员是资源管理流程的责任人，负责对资源管理流程的及时性和有效性负责，全程跟踪资源管理流程过程直至关闭。

南阳移动是云资源管理责任人，对云资源使用的合理性、有效性负责；

资源管理员是云资源容量、分配、质量等管理责任人；

维护经理云资源准备、部署、维护、监控责任人，对云资源正常运行负责。

3.4.3.2.4 监控与告警管理

总体要求

为达到南阳政务云运维管理的可靠性目标，提供功能强大的监控管理系统对云平台进行统一监控及时发现问题，确保政务云平台各个系统功能 7X24 小时稳定可靠运行。监控管理总体要求如下：

1） 针对网络、计算、存储和虚拟层等各系统的不同特点，制定详细完整的常规巡检制度及检查 / 监控规程，确保云平台的高可用性。

2） 监控系统本身的运行情况，每天由值班工作人员进行检查，包括监控软件

公共资源交易平台投标专用

运行情况、部署资源运行状态，确保监控系统的正常运行；

3) 监控系统达到：告警出现时立即通知相应岗位的运维工程师，由对应岗位运维工程师负责故障的排除及判断是否升级故障；

4) 对于监控系统所产生的告警，值班工作人员应按照事件处理流程，做统一记录，并进行故障处理；

5) 监控系统应确保安全管理，操作人员严格按规定执行登录记录、数据备份、系统软件备份齐全；

6) 针对各种维护操作制定相应的岗位职责及管理制度，并通过事后的监督审核确保各项操作得到可靠的执行。对于未能及时对监控系统告警进行处理的行为按照考核制度执行，对于造成严重影响的行为，追究其责任。

平台资源及网络监控

平台资源网络监控应能够监测支撑网络全部物理设备及虚拟设备的当前实时流量、资源使用率、链路状态；对于异常情况，可以根据告警管理当中设定的监控原则及标准，进行主动告警,主要监控内容如下:

1) 设备管理:监控在网交换机、路由器、安全设备及虚拟设备等的设备数量、设备状态、设备标签、型号、IP 地址、设备类型及资产投入使用时间；

2) 拓扑管理：监控网络拓扑及异常变化；

3) 性能管理：监控网络设备的通断、CPU、内存等性能指标

4) 告警监控：监控网络设备的故障，及时产生告警，包括主动轮询、设备 trap 上报等多种方式；

机房监控

1) 机房环境监控系统应达到：温度、湿度、漏水检测监控、闭路监控等测量准确，数量显示稳定;

2) 动力环境监控系统应达到：交流、直流等被测量准确，数据显示稳定；

3) 火灾自动报警系统应达到：无误告警出现，烟感告警反应时间满足要求；

4) 门禁监控系统应达到：门禁出现异常及时通知相应的维护人员，进行故障的判断及维修。

3.4.3.2.5 备份恢复管理

管理目的

为保证政务云上各厅局数据的安全性、完整性，南阳移动维护团队提供数据备份与恢复服务，确保备份数据的完整性，以及在需要进行数据恢复时保障数据的可用性。保证云平台生产环境的稳定性、可靠性，提升云平台系统的可用性。备份与恢复操作的目的在于：

1) 因用户意外删除或误操作导致丢失的数据能得到及时的恢复；
2) 当硬盘等硬件出现故障时云平台服务能得到恢复；
3) 满足灾难恢复的需要；
4) 数据存档，满足业务的查询或国家法律的取证需要。

备份协议管理

备份策略的要求

依据备份数据重要性的不同，采用不同的备份策略。厅局根据业务系统及数据的重要性制定备份策略，运维人员根据业务需求进行实施，备份策略需明确以下内容：

1) 备份内容、备份频率、备份时间窗口
2) 数据丢失容忍时间、数据恢复容忍时间
3) 备份保留期限、备份介质是否异地存储
4) 是否需要归档、归档保留时间、归档确认方式
5) 备份数据可用性确认

备份级别定义

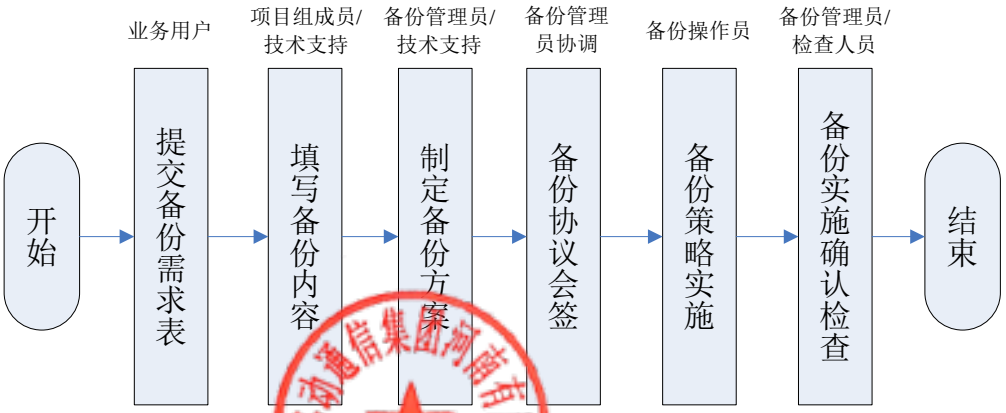
为了保障重要系统获得更高的优先权与数据保护级别，以及控制备份成本，将所有参与备份的数据划分为以下四个级别，从高到低依次是：

- Critical：关键应用
- Core：核心应用
- Important：重要应用
- Normal：其他IT服务器都归入normal组，如文件服务器等

备份协议管理细则

备份协议签署流程如下：

公共资源交易平台技标专用
AE2C15CEC77646E1462A8BC88EA14DB9



备份协议正式签署前要求备份与恢复的方案测试通过。

备份服务内容

数据备份与恢复服务为客户提供了端到端的服务，服务交付人员需要详细了解客户需求，深入分析客户业务系统现状，设计出切实可行的数据备份和恢复方案。

3.4.3.2.6 服务报告管理

在服务期间，对客户的不同服务内容，可根据客户需要提交各类电子文件，主要涉及文档报告如下，业务资源运行报告、故障报告、漏洞扫描报告、安全加固报告等。根据服务内容不同，与客户最终协商确定:

3.4.4 运维服务体系的内容

3.4.4.1 云平台运维管理服务

南阳市政务云，针对机房基础设施、支撑网络及云平台的运维，需要达到高可用、稳定、安全的目标，本项目承诺，以下服务指标作为运维的首要保证目标。

服务可用性

河南移动提供的服务范围内的政务云平台的服务能力，本项目承诺保证各个应用系统可用性不低于 99.99%。

（1）指标定义

1）计划内停机时间

河南移动提前通知甲方且经甲方认定的，为系统正常升级、更新、维护导致的服务停机。

2）服务中断时间

公共资源交易平台投标专用

河南移动提供的机房、网络设备、安全设备、虚拟机、物理机、存储等方面出现的问题引起应用系统失效时间，经甲乙方认定由非河南移动原因引起的系统失效不包含在内。

3）正常服务运行时间

当年总运行时间（按 365 天计算）减去服务中断时间。

4）服务可用性

正常服务运行时间除以该年总运行时间。

（2）指标测量方法

序号	指标名称	测量方法
1	正常服务运行时间	河南移动向甲方及第三方提供测量结果查看接口，并确认检查结果
2	服务中断时间	河南移动向甲方及第三方提供测量结果查看接口，并确认检查结果

3.4.4.1.1 服务响应水平

（1）为最终用户提供技术服务热线(7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法。

（2）在服务期内，提供 7*24 小时的现场和技术支持服务，对故障 15 分钟内响应；30 分钟内到达云中心机房。

（3）在服务期内，7*24 小时运行值班监控，配备具备多年云平台维护经验的运维人员，支持电话、网上值班等响应方式。

3.4.4.1.2 统一服务受理

为达到南阳市政务云运维管理中的可用性的目标，提供 7*24 小时支持服务热线，快速响应客户需求，保证对客户的最终服务质量。并以之作为日常运营过程中相关问题、投诉、建议以及要求提供服务的统一联系点。此外，根据有关紧急情况处理流程，提供值班安排以及紧急联系方式。

该项服务的提供时间为一年 365 天，周一到周日，每天 24 小时。

3.4.4.1.3 SLA 标准

实行 7×24 小时运行维护和响应故障工作，负责政务云平台的故障受理、处

公共资源交易平台技术专用

理、跟踪、结果汇报工作。切实保障政务云平台基础环境的安全、稳定、高效的运行。

对于一般故障要求投标人 30 分钟内进行响应；对于重大故障要求 10 分钟内进行响应；对于特别重大故障要求 5 分钟内进行响应。

3.4.4.2 **运维应急响应**

3.4.4.2.1 流程目的

协助建立、健全南阳市政务云信息安全事件（以下简称安全事件）应急响应体系，规范应急响应工作内容和流程，提高应急响应能力，确保信息系统的安全和业务的连续性，减少安全事件带来的负面影响及损失。

3.4.4.2.2 流程原则

（1）责任人原则

明确信息安全应急响应工作的组织机构，保证各项工作责任到人，信息安全领导小组统一负责安全事件的应急组织和指挥工作。

（2）分级处置原则

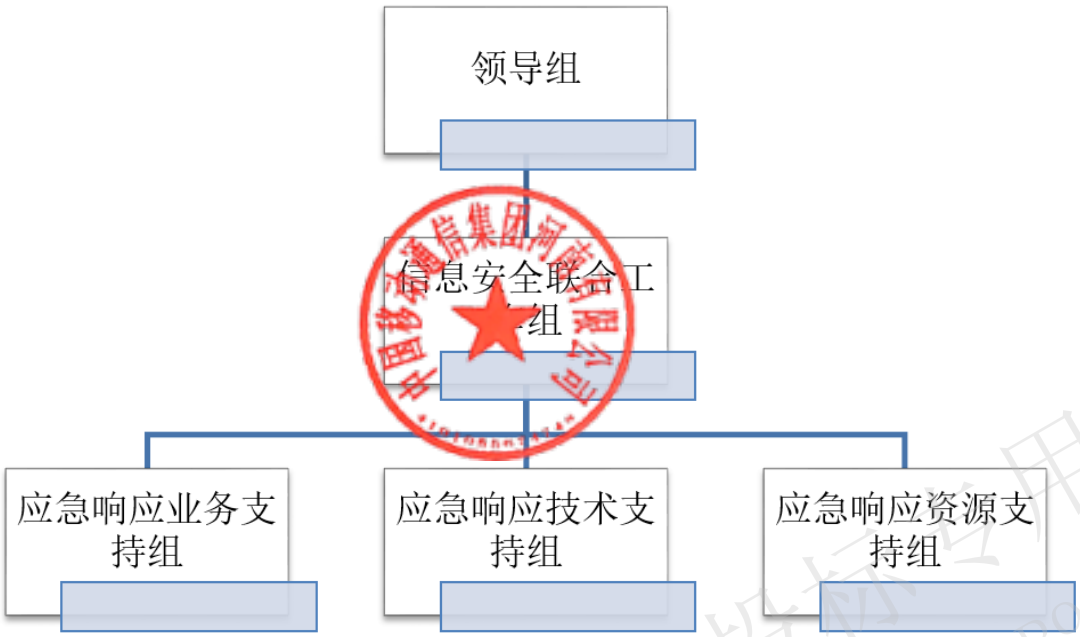
明确安全事件的等级范围、划分依据，制定相应的应急响应流程，确保处置的有效、准确。

（3）有效防备原则

建立安全事件的预案制度。完善安全事件监控和管理机制，积极采取有针对性的应急准备，防备安全事件的恶化。

公共资源交易平台投标专用
AE2C19EC7646E1A62A2BC88EA14B89

3.4.4.2.3 保障组织



岗位职责	职责
领导小组	负责审核和批准信息安全应急响应总体规划、信息安全事件报告。 负责统筹规划信息安全应急基础设施建设。 授权信息安全联合工作组启动特定应急预案。 协调各政务云使用单位配合进行应急方案制定及应急事件处理。
信息安全联合工作组	组建、完善应急响应体系。 定期组织信息系统的风险评估和整改。 定期组织应急预案的演练。 制信息安全事件报告。 负责信息安全事件特定系统应急预案的启动和停止。
应急响应资源支持组	负责应急行动的资源保障工作，包括车辆安排、人员安排等。
应急响应业务支持组	负责制订业务系统应急预案。 负责评估信息安全事件对业务工作所造成的影响。

公共资源交易平台技术专用

	从业务角度，为领导小组及联合工作组决策提供信息和建议。 根据应急响应工作的需要，采取相应的应急处置措施。 编写应急响应业务工作报告。
应急响应技术支持组	负责制订系统技术应急预案。 从技术角度，为领导小组及联合工作组提供信息和建议。 根据应急响应工作的需要，组织施行技术处置措施。 编写应急响应技术工作报告。

3.4.4.2.4 应急预案及演练

应急预案需要在充分调研业务模型的基础上按需量身定制，并以此为依据设计应急演练实战。通过应急演练实战，验证应急预案的预期动作和结果，积累应对云平台突发状况的处理经验。

根据需求，可以不定期组织开展网络与信息系统的应急演练，以检验应急通讯、应急人员、应急设备、应急操作流程的可靠性和可用性。通过应急演练，发现并及时修改应急预案中存在的缺陷和不足，检验各部门的应急保障能力、应急人员对应急响应工作的了解程度和实际操作技能。

各应急响应支持组应定期识别评估职责范围内的业务和技术风险，并根据实际应急响应、系统调整、人员变动、业务变化及应急演练中发现的问题等进行动态维护和更新。信息安全联合工作组负责综合应急预案、应急预案操作办法的动态维护，应急响应技术组、业务组负责特定系统应急预案的动态维护。

3.4.5 人员培训

云服务商要按计划组织培训，培训对象为甲方及甲方最终用户，培训内容包括服务流程和服务资源使用方法等。

3.4.5.1 培训目标

人员培训作为本项目实施的一个重要环节，对整个项目至关重要。因此，我投标方对培训工作极为重视。为了确保系统在使用中稳定、高效率的工作，我投标方在对项目中的各系统技术特点、客户人员状况以及项目实施计划进行具体分析的基础上，针对各系统的管理、维护、应用以及日常故障的处理，为不同人员提供了一系列行之有效的培训实施方案。并针对此次工程的特点设计了专有教材，

结合具有丰富教学经验的教员进行培训。

通过培训要达到以下预期效果：

使系统的业务操作用户，即业务操作人员掌握与自己工作相关的应用系统的使用方法和操作技巧。使用户能通过使用实际的应用系统提高工作效率，从而为项目的成功提供应用上的保障。

使系统的技术人员，即系统管理员、运行维护专业技术人员了解和掌握本项目中会使用到的相关技术：包括应用系统安装及初始化设置技术、系统支撑环境软件设置安装技术、数据交换与共享接口管理技术等，从而为项目的成功提供技术上的保障。使系统管理人员和技术人员，至少达到能独立安装、配置、操作，能独立分析、判断、解决、排除系统一般故障问题。

使参与项目的管理人员、项目负责人、高级工程师（负责系统的需求分析、体系设计等）、质量控制人员能获得标准科学的和规范一致的管理方法，包括项目管理方法、需求分析方法、质量管理方法等，管理人员通过统一的、规范的知识构成与管理体系对项目进行日常管理和监督指导，为项目的成功提供管理上的保障。

增加系统的系统管理人员、运行维护专业技术人员、系统最终用户的知识储备与系统高级技术应用能力，特别是提高一线用户（员工）的 IT 技能，使其具备更大的竞争力，从而提高整个系统从业人员素质。

3.4.5.2 **培训对象**

在系统投入正常运行时，系统的运行操作、管理人员的主体人员应是用户方的有关技术人员及业务人员，所以培训系统的有关技术人员及业务人员，使其达到应有的水平是我们在系统实现过程中一个重要方面。

本项目的培训范围包括：所有需要应用系统进行业务操作的人员及业务管理层领导，按照人员使用系统的方式，可分为省市县三级网络管理人员、项目管理人员、系统管理人员、系统维护人员、云平台最终用户和开发人员。

培训将按照用户的时间安排分次分批进行。

具体按如下几类人员进行培训：

（1）系统管理人员培训

通过对项目管理人员、系统管理人员的培训，使其清晰地了解云平台的设计

理念和设计方法，掌握云平台的整体结构，以及各类云资源的申请、审核、开通、回收等管理流程。

项目管理在项目建设过程中主要参与全过程实施的各专业工程师与技术开发人员和系统维护人员，通过培训，掌握系统的基本维护和日常管理工作，当系统出现一般性问题时，通过系统管理人员能及时解决问题，不影响系统的使用。

（2）系统维护人员培训

通过对系统维护人员的培训，使其切实理解和掌握云平台的相关技术知识，能够熟练地维护云平台，快速定位和解决系统出现的问题，保证云平台服务期间正常运转，并持续提高运维服务质量。

培训系统的日常维护工作，使系统运维人员有能力维护本系统。能够熟练掌握系统的使用，熟悉业务，能在系统使用上给其他工作人员以帮助，对于自己负责的运维内容有维护的能力。

（3）最终用户培训

针对甲方最终使用政务云服务的人员组织云服务培训，培训内容包括云服务介绍、业务上云流程、应用安全责任界面等，帮助最终用户了解云服务商所提供的服务内容，便于用户的业务能够顺利的迁移上云。

3.4.5.3 **培训形式与内容**

根据培训的计划对用户方项目核心人员进行项目的预培训、过程培训等，在项目的建设初期和项目的进行中对相关人员进行培训，安装调试前会对专业技术人员进行培训，在系统升级和其他改动较大的情况下均要进行相关的培训。总之，培训是贯穿整个系统建设全过程的一件非常重要的工作。

为避免培训影响正常的业务工作，我们可以根据项目进度安排，选择统一安排时间对用户进行分批集中培训，而且所有的培训工作都可以在用户现场或单位所在地举行。

基于以往培训经验，在本项目的培训中还可以采用多样的培训形式。通过将培训资料放在网络环境、建立电子化的多媒体教材、知识库等方式，提供网络培训环境，使用户可依赖网络培训环境进行自主学习和互动式的在线培训。

在本项目中，负责系统运维的技术人员都需要具备计算机系统的基本操作能力，达到计算机网络系统维护人员的素质要求，能够承担本工程中各类软硬件设

公共资源交易平台投标专用

备的日常操作管理与维护，并对一般性故障进行诊断、排除及恢复。

（1）现场培训

现场培训旨在针对不同的用户、用户工作、用户环境提供大量小规模、有针对性甚至点对点的系统用户培训。这种培训的特点是针对性强、直观、方式灵活，而且与实际结合紧密，用户在培训中的问题可以及时得到解答。

在系统安装、调试时我们将邀请用户的技术人员参与系统的安装、调试等各项工作，并在实施地点进行现场安装、配置、诊断、管理、维护等方面的培训。

现场培训是为技术人员提供的培训，培训的范围包括系统平台、应用平台、应用软件等的安装调试和管理维护。

（2）集中培训

集中培训是指在用户指定的培训地点实施，并在专门一段时间内进行的技术传授。这种培训方式的优点是，课程内容专业，授课教师队伍精良，针对性强。由于培训时间有保障，所以培训效果也会非常好。

该种形式的培训适用于领导干部、技术人员和业务工作人员在应用软件操作、管理、维护等方面，培训内容全部为本次项目编写的专门教材，由我公司提供，培训讲师全部具有三年以上培训经验，并参与项目实际开发。

3.4.5.4 **培训计划**

结合南阳市政务云项目建设技术覆盖范围广泛的特点，本次项目将主要采用分期集中培训及现场培训等多种方式。现场培训结合项目实施中各个不同阶段，为确保用户方人员能够对硬件设备、软件进行基本的维护和一般故障的排除，

培训开始前我们向客户提供详细的培训计划安排，用户对培训计划审核同意后，我司进行培训计划实施。

（1）政府领导云基础知识及应用培训，培训时长 0.5 天，培训内容：云计算概述与云计算应用；云计算由来；云计算优势；云计算的应用场景。

（2）信息化部门层面的云平台、云资源管理培训，培训时长 2 天，培训内容：云基础架构介绍及实操-OpenStack 介绍;实操使用 FP，管理相应服务器，网络，存储，实现云基础架构；了解云业务迁移理论，手动进行云业务迁移实操；云平台管理及运维。

公共资源交易平台技术专用

3.5 故障处理方案

我方承诺在签订合同后，实行 7×24 小时运行维护和响应故障工作，负责政务云平台的故障受理、处理、跟踪、结果汇报工作。切实保障政务云平台基础环境的安全、稳定、高效的运行。

对于一般故障要求投标人 30 分钟内进行响应；对于重大故障要求 10 分钟内进行响应；对于特别重大故障要求 5 分钟内进行响应。

故障处理方案应从故障处理的流程、网络故障处理、服务器故障处理、业务系统故障处理等方面来阐述说明。

3.5.1 故障处理的级别

我方具体服务时限根据相应服务级别的要求履行，如下表：

序号	故障级别	故障描述	响应要求	解决时限要求
1	一级	系统中的关键设备或应用软件出现故障，导致系统瘫痪，重要核心业务无法开展，或出现严重信息、数据出错、重要数据丢失，甚至引起纠纷，给招标人带来非常严重的损失	自故障申报时起，5 分钟之内响应	自故障申报时起，2 小时内解决问题；如需原厂家外地技术专家上门解决，4 小时内解决问题
2	二级	系统中的主要设备或应用软件出现故障，或处理性能严重下降，基本业务受到严重影响，如果不立即排除故障、恢复业务，会给招标人带来严重的损失	自故障申报时起，15 分钟之内响应	自故障申报时起，3 小时内解决问题；如需原厂家外地技术专家上门解决，6 小时内解决问题
3	三级	系统的部分操作性能受损，处理部分性能出现	自故障申报时起，30 分钟之内响应	自故障申报时起，8 小时内解决问题；

公共资源交易平台投标专用

		下降，系统功能削弱，但大部分业务运作仍可正常工作		如需原厂家外地技术专家上门解决，12 小时内解决问题
4	四级	系统中发现有故障隐患的报错、或软硬件临时性报错、或某个单项功能出错需要修复。这些故障均在可控制范围内，对基本业务系统运作几乎无影响或影响甚微	自故障申报时起，30 分钟之内响应	自故障申报时起，48 小时内解决问题；如需原厂家外地技术专家上门解决，72 小时内解决问题

故障发生后，无论故障性质及来源，我方将在规定时间内到达现场并作出判断。如属质保范围的故障，将在规定时间内解决。如故障超出质保范围，服务提供商在规定时间内作出故障原因的正确判断并出具故障报告，可视作解决，但如出具故障报告不及时或故障原因判断错误，视作未解决。

故障发生后，我方可通过应急处理技术手段，临时恢复业务正常运行的，该故障报警可以关闭。我方会及时修复故障，招标人将自该故障报警关闭之时起，统一按照四级故障对修复故障进行计时。由于系统 BUG、配件采购、协调外单位、寻求厂家技术支持等原因需要延长期限的，我方将及时说明情况并在时限到期前向招标人提出延期申请，经招标人同意继续延期。

故障解决后，我方将编制故障处理手册、提供故障报告（对故障处理进行总结）、制定此类故障的应急预案并实施，同时提供该故障解决方案的培训。

3.5.2 故障恢复响应

故障等级	故障说明	响应时间	处理时间
一级	一级故障：系统无法使用，影响用户正常使用。 当系统出现下列相当严重的现	≤5 分钟	≤2 小时

公共资源交易平台投标专用

	象时，属一级故障： 系统后台服务器整体瘫痪，全部操作失去响应；系统崩溃、无法进入用户界面；发生间歇性、随机性、重复性的启动或应用退出，无法保障客户业务的正常处理。两个二级故障及以上，升级为一级故障。		
二级	二级故障：整体可以使用，部分出现问题，影响用户的部分业务处理。 当系统出现下列比较严重的现象时，属二级故障： 系统后台出现了部分问题，导致用户使用出现问题；部分功能失效，影响用户使用；系统整体性能严重下降，无法自动恢复正常运行状态；重要数据、参数和配置信息损坏，无法恢复，导致数据及业务记录严重损失。	≤10 分钟	≤2 小时
三级	三级故障：可以使用，出现的问题对用户的业务处理影响不大。当系统出现下列现象时，属三级故障：服务器端或者硬件出现异常，局部功能受限，系统整体仍可正常工作，对客户业务影响不大或存在隐患； 关键备用设施因故障离线，主用设施仍能正常工作；后台日	≤30 分钟	≤4 小时

公共资源交易平台投标专用

	志发现有系统出现问题的趋势，或者已经出现了交易成功率下降客户端性能小幅下降，但不影响使用；系统运行指标（例如： I/O 效率、 CPU 效率）受到直接或间接影响，客户业务处理受小量影响．五个四级及以上，升级为三级故障。		
四级	四级故障：可以使用，不影响业务处理当系统出现下列情况而不影响客户业务时，属四级故障：界面出现显示问题，如 ui 不符合设计；后台系统中有大量的冗余信息，导致空间不足；系统硬件或者软件没有及时升级，不符合安全策略等等。	≤30 分钟	≤4 小时

3.5.3 重大故障现场响应

重大故障现场响应服务是指在客户面临重大故障面前，移动能提供重大故障快速响应和故障根因分析及优化服务，确保客户能够快速恢复业务。移动将提供对故障的根因定位分析服务，并优化故障根因，提高业务连续性。

2、服务内容

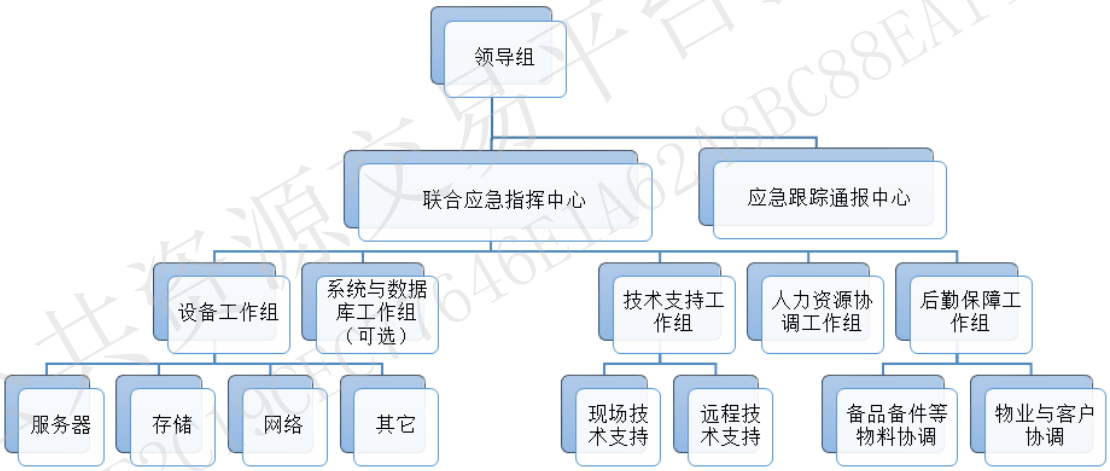
针对职责范围内的重大故障现场响应服务内容主要包括以下几部分：

- 重大故障发生时，移动提供快速响应服务，确保故障能够得到快速处理。
- 重大故障时，运维工程师会保存故障相关信息，为后续故障根因分析和优化提供资源。
- 重大故障处理前，运维工程师会制定解决方案优先恢复业务，保障业务连续性。
- 恢复业务后，根据之前保存得当故障相关信息，进行故障根因分析。
- 建立具有监测故障、及时解决故障的机制。

公共资源交易平台投标专用

- 通过规范故障管理，确保故障得到快速有效地处理，尽快恢复正常的业务运行，将故障对服务使用方的影响降到最小。
- 根据事件管理过程的要求建立与故障管理过程一致的活动，包括故障受理、分类和初步支持、调查和诊断、解决、进展监控与跟踪、关闭等。
- 对运行保障服务过程中的故障进行分类，类别应包括：基础设施组件类、网络系统类、主机系统类、终端系统类、数据库系统类、中间件系统类、存储与备份系统类、安全保障系统类、机房环境类、应用类、文档类等。
- 根据与服务使用方达成的服务协议要求，建立故障的自动升级机制，在规定时间内没有处理完成的故障，自动升级为上一级的故障。
- 故障修复完成后，提供故障分析报告及后续优化建议。

3.5.4 故障应急预警组织



组织架构中人员职责

领导组：

a）负责统一领导与重大决策；

b）根据应急处理进展与问题，给出应急处理要求与指导意见；

联合应急指挥中心：

a）建立健全应急管理体系，持续完善应急预案，组织开展应急演练，提高预案的完备性和有效性；

b）审定重大突发事件的应对策略、处理流程和快速响应机制，保证突发事

公共资源交易平台投标专用

件信息传递、指挥调度和处理过程的准确性与时效性，确保突发事件得到快速、有效、有序地处理；

c）审定信息中心重大突发事件处理工作流程，决策启动应急预案；

d）指挥、协调重大突发事件的处理，组织应急资源，快速应急响应和应急恢复，并对外通报相关事项。深刻分析事件症结所在，采取有效手段杜绝事件再次发生；

e）评估和认定重大突发事件的影响，及时向有关部门通报情况；

f）根据重大突发事件发生场景和处理过程，补充、完善应急预案；

g）对应急预案进行管理授权，输出最终的确认和审批；

h）评估重大突发事件处理流程，持续完善中心应急管理工作；

i）部署安全意识教育工作，培植安全文化氛围；

应急跟踪通报中心：

a）负责监视故障、告警发生情况，发生重大故障时，第一时间向指挥中心汇报，并定时向指挥中心汇报故障发生与处理情况；

b）及时跟进各故障抢修的进展情况，对于长时间没有处理或处理较慢的故障，要向指挥中心报告，且向一线抢修人员询问不抢修或施工缓慢的原因，并记录；

c）根据统一汇报模板，定时向各层面汇报应急处理进展；

设备/系统与数据库/动力工作组：

a）输出产品应急解决方案，做好应急工作准备；

b）负责应急解决方案执行；

c）定时向应急指挥中心与应急跟踪通报中心汇报应急处理进展；

技术支持组：

a）对应急方案的故障处理给予技术授权；

b）负责对现场应急处理技术保障；

c）拉通一线与二线技术专家，对疑难问题输出现场技术解决方案并予以实施指导；

人力资源协调工作组：

a）统一部署人力资源；

公共资源交易平台投标专用

b）响应人力资源求助申请，做好人力资源协调工作；

后勤域保障工作组：

a）根据应急工作要求，做好应急后勤保障准备工作，包括物料、各接口协调工作准备等；

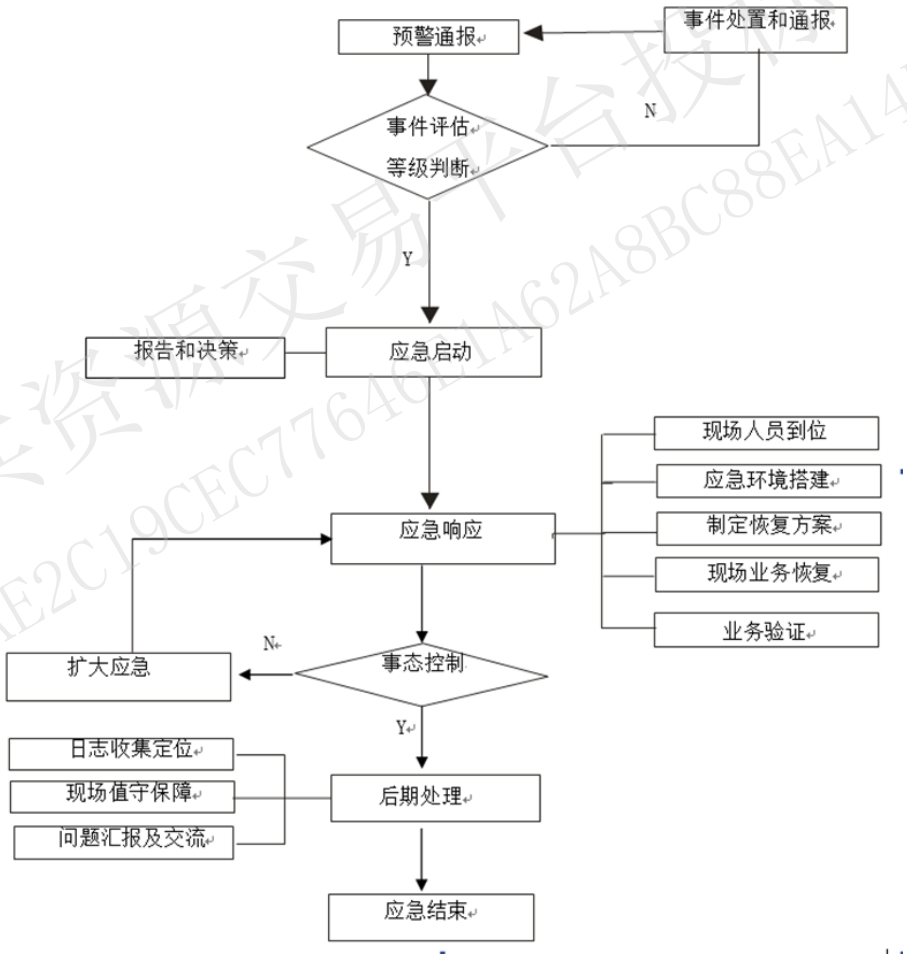
b）收集预警、灾情信息并及时上报；

c）加强通信应急车辆、应急装备、备品备件和仪表工具、抢修物资的统一调度与管理工作；

d）负责物业、客户等沟通与协调工作。

3.5.5 故障处理的流程

3.5.5.1 故障应急处理流程图



3.5.5.2 远程故障处理

远程故障问题处理服务包含两部分内容，技术咨询和故障问题处理。

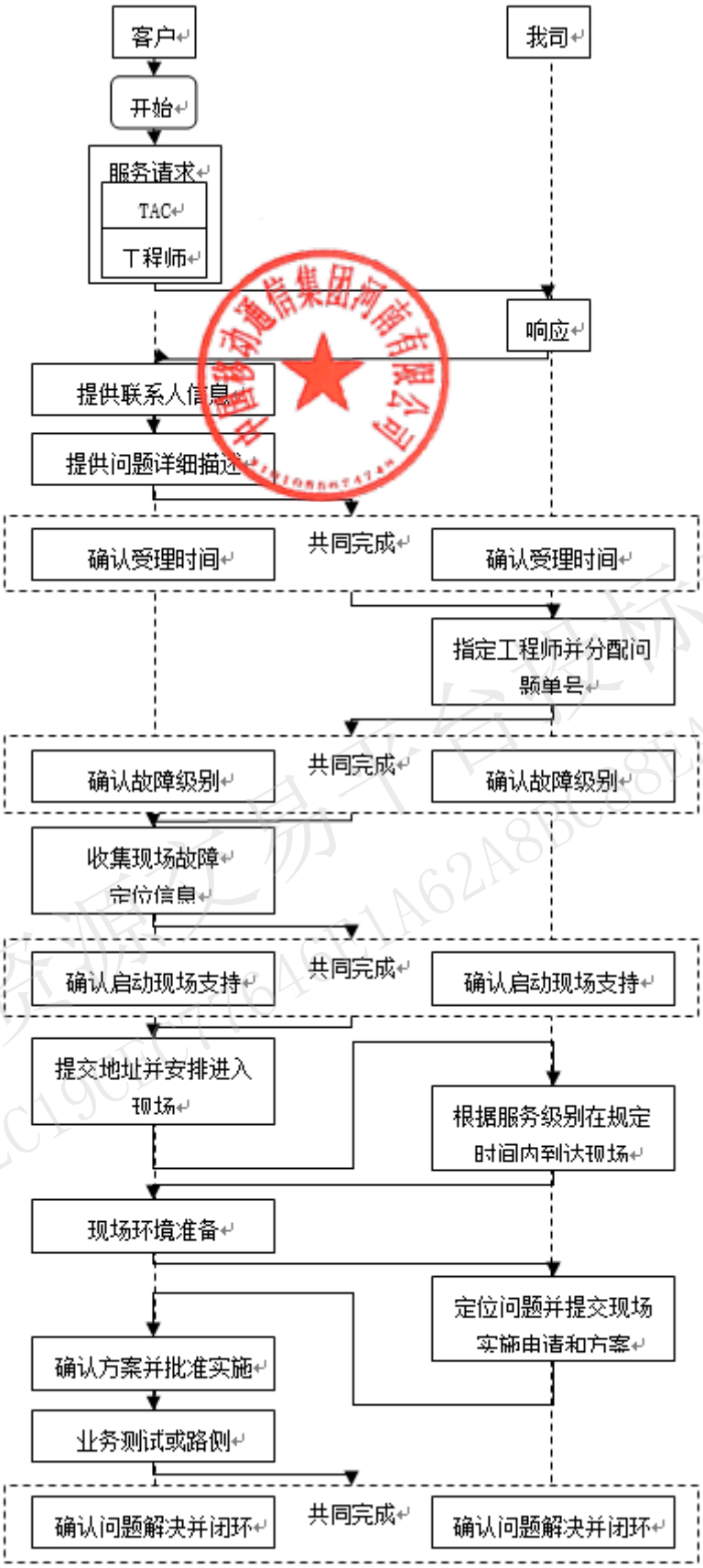
技术咨询：是指我司向南阳市政务云平台提供的针对您在日常运维过程中遇

公共资源交易平台投标专用
AE2CJ9CEC77646D1A62A8BC88EA14DB9

到的有关设备功能、规格、操作以及配置方面的问题的答复，不包括网络优化方面的问题咨询。在接收到南阳市政务云平台的服务请求后（服务器故障处理、网络故障处理、业务系统故障处理），我司会就该咨询请求进行分析，分析后的答复会通过电话、传真、或电子邮件等方式提供给您。

故障问题：处理指我司对南阳市政务云平台提交的设备或网络的问题（不包括网络性能优化的问题）进行故障根因分析，并提供问题解决方案。在故障问题处理过程中，南阳市政务云平台负责提供必要的信息和实施解决方案，我司提供远程协助。故障处理流程如下图：

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9



远程技术支持服务包含技术咨询和故障问题处理。

公共资源交易平台投标专用

（1）技术咨询

技术咨询是指我方提供的针对南阳市政务云平台在日常运维过程中遇到的有关设备功能、规格、操作以及配置方面的问题的答复，在接收到南阳市政务云平台工程师的服务请求后，我方会就该咨询请求进行分析，分析后的答复会通过电话、传真、或电子邮件等方式提供给南阳市政务云平台的工程师。

（2）故障问题处理

故障问题处理指我方对南阳市政务云平台工程师提交的南阳市政务云平台设备问题（网络故障处理、服务器故障处理、业务系统故障处理）进行故障根因分析，并提供问题解决方案。在故障问题处理过程中，问题申报人员负责提供必要的信息和实施，提供远程协助。

（3）远程紧急故障支持服务

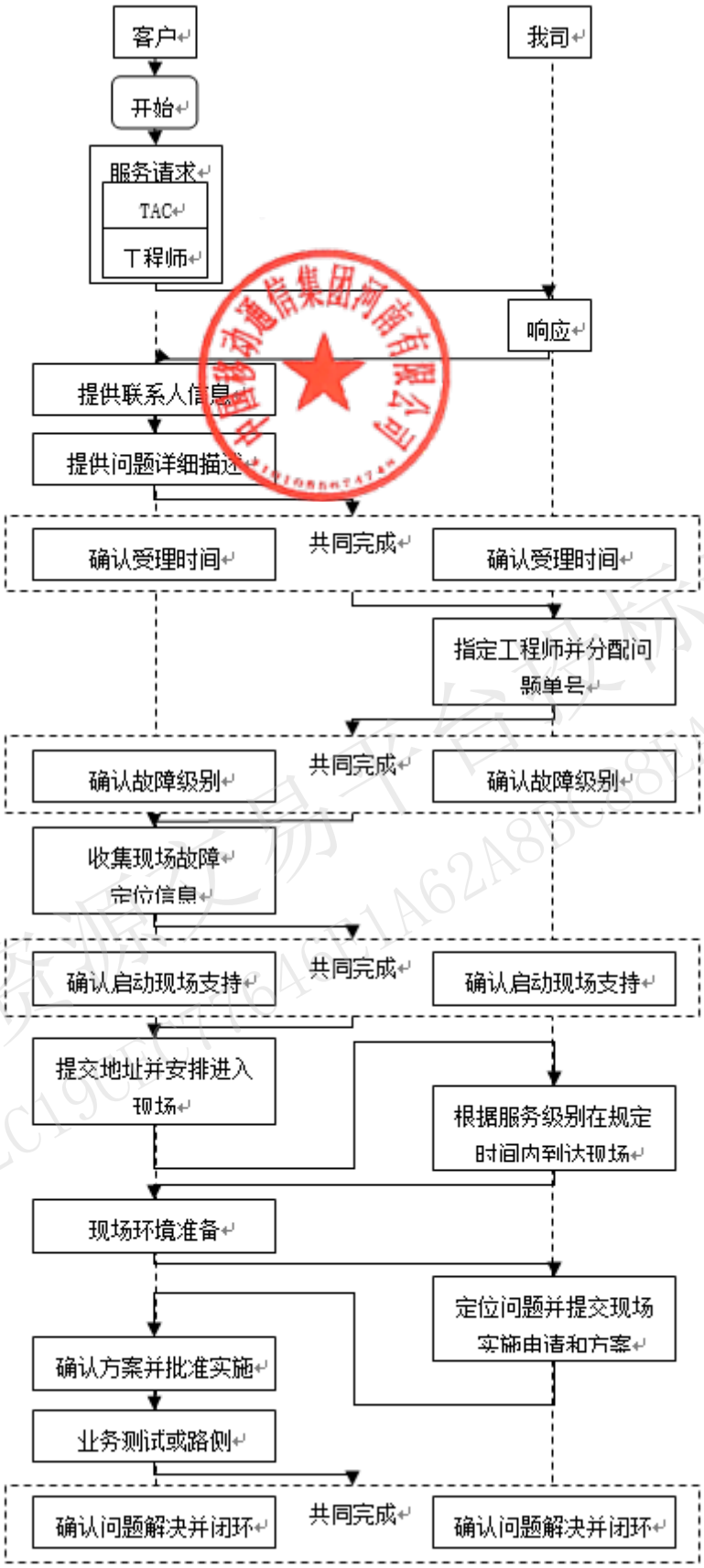
远程紧急故障支持服务是指我方在紧急故障情况下为帮助南阳市政务云平台尽快支持业务而提供的远程支持服务。在紧急故障情况下，我方提供 7×24 的紧急故障支持服务，协助客户尽快将业务支持到故障前的状态和南阳市政务云平台可接受的状态。南阳市政务云平台通过电话方式向我方申请紧急故障支持服务，我方工程师将通过电话或远程连接的方式为客户提供服务，协助客户实施支持方案尽快支持业务。

3.5.5.3 **现场故障处理**

在南阳市政务云平台项目上线后出现南阳市政务云平台相关的故障（网络故障处理、服务器故障处理、业务系统故障处理）时，我司根据项目故障类型，第一时间响应故障处理诉求，按照约定的服务内容提供对应的服务。

对于现场服务，需要南阳市政务云平台指定有相应资格的运维人员在现场配合我司工程师，以提供所需的信息和帮助，并确保我司工程师可以方便地进出站点、获取操作相应的设备的权限和工作环境的安全。服务流程如下图所示：

公共资源交易平台投标专用



（1）现场问题处理服务

公共资源交易平台竞标专用

现场问题处理服务是指我方工程师到达南阳市政务云平台项目现场进行信息收集、问题分析、故障诊断、问题解决方案实施的支持服务。当我方接到南阳市政务云平台的现场问题处理服务申请后，在确认现场服务内容和必须的信息后，我方会安排工程师前往项目现场，按照约定的服务内容提供对应的服务。对于现场服务，我方工程师全力配合南阳市政务云平台指定有相应资格的运维人员在现场处理及操作。期间需南阳市政务云平台提供所需的信息和帮助，确保我方工程师可以方便地进出站点、获取操作相应的设备的权限。

（2）现场紧急故障支持服务

现场紧急故障支持服务是指在紧急故障情况下，我方为了帮助南阳市政务云平台项目尽快支持业务和减少影响而提供的现场支持服务。

当我方接到南阳市政务云平台的现场紧急故障支持服务申请后，在确认现场服务内容和必须的信息后，安排工程师前往项目现场，分析紧急故障情况，采取各种可能的措施向南阳市政务云平台提供有效的支持方案，并协助南阳市政务云平台尽快将业务支持到故障前的状态或用户可接受的状态。同时还会协助南阳市政务云平台采取必要的预防措施以防止紧急故障情况的再次发生。

在紧急故障现场支持的过程中，我方工程师全力配合南阳市政务云平台指定的一名有相应资格的运维人员在现场处理及操作。期间需南阳市政务云平台提供所需的信息和帮助，确保我方工程师可以方便地进出站点、获取操作相应设备的权限。

3.5.6 网络故障处理

- **日常巡检**

1、服务描述

网络系统例行巡检是网络日常维护的一个重要组成部分，定期对机房进行一次巡检，由网络工程师对网络进行分析，借助网络例检可以及时发现故障的先期征兆，使得我们可以提前将故障排除，减小网络故障发生频率。网络例检将采用检查工具，并结合日志服务器和人工分析生成例检报告。

2、服务内容

将巡检分为日巡检、周巡检、月巡检和节前巡检，并及时提交巡检报告。对于巡检中发现的问题，第一时间上报并提出解决建议和方法

公共资源交易平台技标专用

制定巡查内容和巡查计划。

对网络系统中的交换机各种运行状态、环境、指标进行检查

对网络系统中的防火墙各种运行状态、环境、指标进行检查

对网络系统中的负载均衡器运行状态、环境、指标进行检查

对网络系统中的安全设备运行状态、环境、指标进行检查

巡查异常内容的可整改方案提供。

巡检异常内容的整改实施或跟踪。

对于工作中涉及到对设备配置项的变更，需要遵守相应的变更流程，对于检查到的异常事件需要按照事件&事故管理流程进行处理，工作中需要遵守指定的管理办法。

- **告警处理**

1、服务描述

告警处理是通过实时监控软件对网络设备各种运行状态、运行环境、资源等监控，若与预设参数值变化，立即通过监控软件或通过手机短信的方式，发送给甲方管理人员、网络维护人员。网络运维人员在收到告警后立即收集故障信息，登录设备进而检查处理。

2、服务内容

针对网络和安全设备确认告警项并进行相应的内容收集，支撑后续的告警监控和相应的告警处理。告警处理的主要活动内容如下：

告警内容梳理，收集设备告警信息。

增加&减少时相应可支撑配置的配合。

告警查看&处理，收集和掌握告警的处理方式，并进行相应告警的处理。

告警升级，对于收集的告警进行分类，确认那些告警需要升级。

监控报告，对于告警的监控和处理状况输出相应的告警分析报告。

如果告警需要版本解决或配置更改，需要遵守对于工作中涉及到对设备配置项的变更，需要遵守相应的变更流程，对于检查到的异常事件需要按照事件&事故管理流程进行处理。

- **性能监控**

1、服务描述

公共资源交易平台投标专用

对所有网络设备的性能使用网络工具或脚本进行深度检查，包括 CPU、内存、连通性、连流量带宽、错报率、传输延迟和延迟抖动等，并提交性能分析报告。对发现的异常情况提出优化建议。

2、服务内容

- 对交换机 CPU、Memory 使用率的的监控，超过预定阀值触发告警。
- 对交换机物理端口的流量带宽的使用率实时监控，超过预定阀值触发告警。对交换机的物理端口的错报率、传输延迟进行实时的监控，超过预定阀值触发告警。
- 对防火墙的 CPU、Memory 使用率的的监控，超过预定阀值触发告警。
- 对防火墙的物理端口的流量带宽的使用率实时监控，超过预定阀值触发告警。
- 对防火墙的并发连接数、转发时延实时监控，超过预定阀值触发告警。
- 对安全设备的 CPU、Memory 使用率的的监控，超过预定阀值触发告警。
- 对安全设备的并发连接数实时监控，超过预定阀值触发告警。

➢ **故障处理**

1、服务描述

故障处理过程分为：故障受理，故障信息收集，故障分析，故障恢复处理，故障报告。

2、服务内容

故障受理是指通过电话告知，告警短信或监控软件时发现出现故障，网络维护人员立即参与故障处理。

故障信息收集的内容有：

- 记录具体的故障现象、故障时间、配置信息。
- 记录完整的网络拓扑，包括组网图、端口连接关系、故障位置。
- 记录现场采取的故障处理措施（比如配置操作、插拔线缆、手工重启设备）及实施后的现象效果。
- 记录故障处理过程中配置的所有命令行显示信息。
- 搜集设备日志信息和 diag 信息
- 记录抓取的报文信息、Debug 开关打印信息、主控板与网板持续异常重

公共资源交易平台投标专用

启的串口输出信息。

- 记录设备故障时单板、电源、风扇指示灯的状态，或给现场设备拍照记录。
- 故障分析：
- 通过收集的综合信息，分析出故障类型，如硬件故障、软件故障、链路故障、安全策略、负载均衡策略、路由等。
- 故障恢复处理：
- 处理硬件类的故障，常用方法有：更换光模块、隔离故障单板（将业务流量调整到正常单板）、更换故障单板
- 处理软件类的故障，常用方法有：重启故障设备协议，调整业务流隔离故障设备，升级软件版本。
- 处理链路类的故障，常用方法有：检修故障链路、调整业务流隔离故障线路。
- 处理其他类的故障，常用方法有：调整安全访问策略、调整路由配置、调整 vlan 配置、调整负载均衡策略配置等
- 故障报告：
- 针对故障解决之后，详细分析故障，提出优化建议如何避免同类故障再次发生，并在故障后 24 小时内上交有关部门。

➢ **配置变更**

1、服务描述

对需要进行网络设备的配置进行调整、修改、增删等工作，经审批后方可实施配置变更。并且配置变更前先进行配置备份和准备回退方案等工作，若变更过程中影响到业务系统运行，应立即回退。在配置变更后务必再次检查系统运行状态。

2、服务内容

- 对交换机路由的调整，包括对动态路由的调整，对静态路由的调整，对路由 cost 值得调整，路由策略的调整，动态路由的邻居认证等。
- 对交换机 vlan 的调整，包括 access 模式,trunk 模式和 vlan 透传
- 对交换机端口的调整，包括双工、速率、vlan-id、端口模式等

公共资源交易平台投标专用

- 对防火墙的访问控制策略的调整，包括通过源 IP，目的 IP，TCP/UDP 端口对 IP 互访进行控制
- 对防火墙的安全域的调整，即安全域的优先级的调整
- 对防火墙的 NAT 的调整，包括静态 nat 和动态 nat 的调整
- 对安全设备策略的调整

➢ **业务资源发放支持**

1、服务描述

在政务云运营维护中，各部门之间、各业务局委办之间需要相互沟通、协调、配合，通过调试设备、更改运行参数、更改环境参数等，达到在保证安全的情况下，互联互通之目的。

2、服务内容

- 网络/负载均衡配置及策略调整： IP、VLAN 规划管理，端口配置、路由策略、QOS 策略、负载均衡策略等
- 业务发放/上线/割接网络打通、调测配合
- 安全合规、审计、加固配合与实施

3.5.7 服务器故障处理

1、服务描述

对服务器和存储设备例行巡检是系统日常维护的一个重要组成部分，定期对政务云机房进行一次巡检，对服务器和存储进行分析，借助例检可以及时发现故障的先期征兆，使得我们可以提前将故障排除，减小系统故障发生频率。生成例检报告。

2、服务内容

将巡检按照设备厂商推荐周期和内容进行，并及时提交巡检报告。对于巡检中发现的问题，第一时间上报并提出解决建议和方法

- 制定巡查内容和巡查计划。
- 对系统中的服务器和存储硬件外观检查，如设备位置变更、清洁度、风扇运行、告警指示灯、线缆状态、滤网状态和液晶面板等
- 对系统中的服务器设备各种运行状态、环境、指标进行检查

公共资源交易平台投标专用
AE2C19C4C77646E1A62A8BC88EA14DB9

- 对系统中的存储设备各种运行状态、环境、指标进行检查
- 巡查异常内容的可整改方案提供(由设备厂商负责)。
- 巡检异常内容的整改实施或跟踪。

对于工作中涉及到对设备配置项的变更，需要遵守相应的变更流程，对于检查到的异常事件需要按照事件&事故管理流程进行处理，工作中需要遵守指定的管理办法。

➢ **告警处理**

1、服务描述

告警处理是通过实时监控软件对系统中的服务器和存储设备的各种运行状态、运行环境、资源等监控，若与预设参数值变化，立即通过监控软件或通过手机短信的方式，发送给甲方管理人员、系统维护人员。系统运维人员在收到告警后立即收集故障信息，现场检查和登录设备进而检查处理，对不可处理问题协调设备厂商进行处理。

2、服务内容

针对服务器与存储确认告警项并进行相应的内容收集，支撑后续的告警监控和相应的告警处理。告警处理的主要活动内容如下：

- 告警内容梳理，收集设备告警信息。
- 告警策略维护、稽核。
- 告警查看&处理，收集和掌握告警的处理方式，并进行相应告警的处理。
- 告警升级，对于收集的告警进行分类，确认那些告警需要升级。
- 监控报告，对于告警的监控和处理状况输出相应的告警分析报告。
- 告警策略优化。
- 告警管理流程优化。
- 告警处理手册编写与优化

如果告警需要版本解决或配置更改，需要遵守对于工作中涉及到对设备配置项的变更，需要遵守相应的变更流程，对于检查到的异常事件需要按照事件&事故管理流程进行处理。

➢ **性能监控**

1、服务描述

公共资源交易平台技术专用

对所有服务器和存储设备的性能使用监控软件进行监控，并提交性能分析报告。

2、服务内容

- 对服务器和服务器的运行状态如电源、电池、风扇、各种指示灯的监控 。
- 对服务器和存储利用监控软件针对 CPU、Memory 使用率的统一监控。
- 对服务器的本地磁盘磁盘空间、磁盘读写延迟、RAID1 的监控。
- 对服务器的物理网络端口的带宽使用率监控。
- 对存储设备的 CPU 板、内存板、Cache 使用率的监控
- 对存储设备的前端端口板和后端端口板的繁忙度、IO 时延、IOPS 的监控
- 对存储设备的存储容量剩余率的监控
- 对光纤交换机的光纤端口、TRUNK 口流量的监控

➢ **配置变更**

1、服务描述

对需要进行服务器和存储设备的配置进行调整、修改、增删等工作，经审批后实施配置变更。并且配置变更前先进行配置备份和准备回退方案等工作，若变更过程中影响到业务系统运行，应立即回退。在配置变更后务必再次检查系统运行状态。

2、服务内容

- 协调服务器设备厂商对部件进行更换，如 CPU、内存条、磁盘、HBA 卡、电源、风扇等
- 对服务器本地磁盘镜像的创建、拆分、更换等调整
- 服务器修改调整网卡 IP 地址、掩码、双工和速率的调整
- 服务器的多路径软件模式调整，如双活、failover。
- 服务器逻辑卷的调整，如空间扩容，空间紧缩、条带、raid5 等
- 协调存储设备厂商对部件进行更换，如 CPU、内存条、光模块、前端端口板、后端端口板、电源、电池、风扇等
- 协调存储设备提供商配合调整,如存储交换机 ZONE 划分、底层存储卷分配，LUN masking、LUN mapping、HBA 卡扫描新划分的 LUN 等

➢ **业务发放实施支持**

公共资源交易平台投标专用

1、服务描述

在政务云运营维护中，各部门之间、各业务厂商之间需要相互沟通、协调、配合，通过调试设备、更改运行参数、更改环境参数等，达到在保证安全的情况下，为业务提供基础应用平台之目的。

2、服务内容

- 服务器安装配置本地磁盘为 RAID1 模式，以保证高可用性
- 服务器安装配置本地物理网卡，要求与两台物理交换机连接，保证网络的高可用性
- 协调监控管理人员沟通协调部署告警策略，如 CPU、MEMORY、crontab 剩余数、swap 使用率、磁盘 IO、网络连接数、登录有效性、可用服务 IP、逻辑卷
- 协调存储设备厂商配合完成存储设备给服务器 LUN 的划分工作。

3.5.8 业务系统故障处理

1、服务描述

负责配合各上云单位处理上云业务系统故障。

2、服务内容

一般故障处理流程

- 常规的故障一般来源于值班人员接收到用户报障以及机房的日常巡检发现。用户的保障热线电话：0377-83889600；
- 值班人员对电话保障酌情处理，如是简单操作问题可以直接电话沟通，如确认是设备或系统故障，应将故障信息尽快上报给政务云项目组；
- 政务云项目组工程技术人员在接收到故障信息后,尽快到达现场确认故障情况和设备状态；
- 工程技术人员对故照确认后,如可以现场排除的,可以将权相关管，理人员解决,如确认是疑难故障,则应尽快报交厂家技术人员协调解，>接认故障管决后；
- 确认故障解决后，把相关结果反馈给客户，告知其可以继续使用。

公共资源交易平台投标专用
AE2C15CEC77646E1A62A8BC88EA14DB9

系统安全故障处理流程

- 操作系统故障一般来自用户报告和巡检发现；
- 值班人员针对用户反馈检查日志，查看虚拟机是否中毒，并选择相应的措施；
- 若发现有病毒，且已经清除，请用户自行检查操作系统使用情况，排查原因，网络部提供必要定位和协助；
- 若发现病毒，且清除失败，网络部协助客户定位病毒信息，并1小时内通知用户查杀，若2小时内用户未反馈，强制关闭虚拟机。问题闭环；
- 若未中毒，请用户自行检查操作系统使用情况，网络部提供必要协助；
- 所有问题闭环后记录处理过程。

3.5.9 故障响应时间

服务内容	级别	描述
热线受理	7×24	7×24：提供 7*24小时 0377-83889600 电话支持
远程故障处理	7×24	7×24：周一至周日,00:00～24:00（全天候，节假日无休）
现场技术支持	7×24	7×24：周一至周日,00:00～24:00（全天候，节假日无休）
紧急故障现场支持	7×24立即出发	7×24：周一至周日,00:00～24:00（全天候，节假日无休）

3.6 应急响应方案

在运维工作中，对故障的处理是非常重要的一部分，我方根据南阳市政务云的业务需要，定制了详细的针对故障处理的运维方案，并对云平台上运行的业务系统出现的故障，提供 7*24 小时的技术响应，配合相关单位及时排除故障。

我方提供系统故障应急处理预案，提供出现问题的快速解决方法，制定完善合理的应急响应方案。

投标人每年应进行不少于 2 次的应急演练。

应急响应方案应从响应时间、电力应急、空调应急、消防应急、网络及系统

公共资源交易平台投标专用

应急、云平台故障应急等方面来阐述说明。

3.6.1 应急响应服务

（1）应急体制和总则

应急领导小组与应急团队：应急领导小组由双方相关人员组成。领导小组组长由采购人相关负责人担任，成员主要为运维团队人员组成。应急团队由多方人员组成，例如运维团队、业主代表、各单位代表、管理组、供应商代表以及其他第三方人员等。

应急领导小组职责：负责编制、修订所辖范围内突发信息网络事件应急预案；牵头与协调相关人员和单位处理各种异常情况；及时组织人员对突发事件进行应急处置；负责组建信息网络安全应急救援队伍并组织培训和演练。

应急团队职责：负责响应应急领导小组的一切要求；根据应急领导小组的指示妥善处理各种异常情况；负责调查和处理紧急事件，及时上报并按照相关规定作好善后工作。一旦发生灾难，由负责人主导，首先保人员安全，其次保关键设备、数据安全，三是保一般设备安全。

（2）预防及响应机制

突发信息网络事件安全预防措施包括分析安全风险，准备应急处置措施，建立网络和信息系统的监测体系，控制有害信息的传播，预先制定信息安全重大事件的通报机制。

建立应急预案库，提高南阳市政务云平台预防应急的效率。通过应急预案库的应急预案，优先恢复对外服务，减少对最终用户的影响，然后在进行故障排查，彻底解决存在问题及后患。

（3）黑客攻击事件

应急措施包含当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告应急领导小组。接报告后，应急领导小组应立即指令维护人员核实情况，关闭服务器或系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登陆账号，阻断可疑用户进入网络的通道。维护人员应及时清理系统，恢复数据、程序，恢复系统和网络正常；情况严重的，应上

公共资源交易平台技术专用

报应急领导小组，并请求支援。处置结束后,维护人员应将事发经过、处置结果等在调查工作结束后一日内报告应急领导小组。

（4）核心设备硬件故障

应急措施包含发生核心设备硬件故障后，维护人员应及时报告应急领导小组，并组织查找、确定故障设备及故障原因，进行先期处置。若故障设备在短时间内无法修复,维护人员应启动备份设备,保持系统正常运行,将故障设备脱离网络，进行故障排除工作。维护人员应在故障排除后,在网络空闲时期,替换备用设备，若故障仍然存在，立即联系相关厂商，认真填写设备故障报告单备查。事态或后果严重的，及时报告应急领导小组。如有必要，及时通知用户相关负责人及相关领导。

（5）大型灾难紧急行动方案

发生水害、火害等自然灾害时报警措施：严格遵守火警处理流程；关闭供电总闸；启用灭火设备进行灭火，并打火警电话 119；全力保护重要的数据备份，并转移到安全地点；完全灭掉各种明火；尽量保护好火灾现场，协助有关方面勘察分析火灾发生的原因、造成的损失、提出批评防范措施和需要改进的地方；对发生火灾造成的损失、原因等做好记录，经部门负责人、联社领导审阅后，向上级主管部门全面汇报。

防雷措施：为防止高压雷电波侵入设备，可在设备前端采用多种防雷装置。例如，在网络设备前设三级避雷装置可有效分流限压，防止感应雷电波的侵入，三级避雷装置指电源端、UPS（译文：不间断电源）端、服务器端。防雷措施主要针对直击雷和感应雷,一般做法是装设避雷针。由于雨季约在 4 月——8 月，在这段期间必须每月做一次防雷设备的测试。除 4 月——8 月外，必须 4 个月做一次防雷装置的测试。

断电处理措施：市电供电中断后，运行人员应立即切换到备用电源-UPS。运行人员应立即查明原因，并向上一级汇报。立即致电资源调度组长，并协助恢复电源。

设备入水措施：发生设备入水后，可由服务工程师向有关部门汇报入水后机器情况。汇报后主要由服务工程师组织人力，进行实施。环境正常以后，将硬件设备恢复到原来状态，若数据有错误，利用最近日期的数据备份磁带进行恢复。

公共资源交易平台投标专用

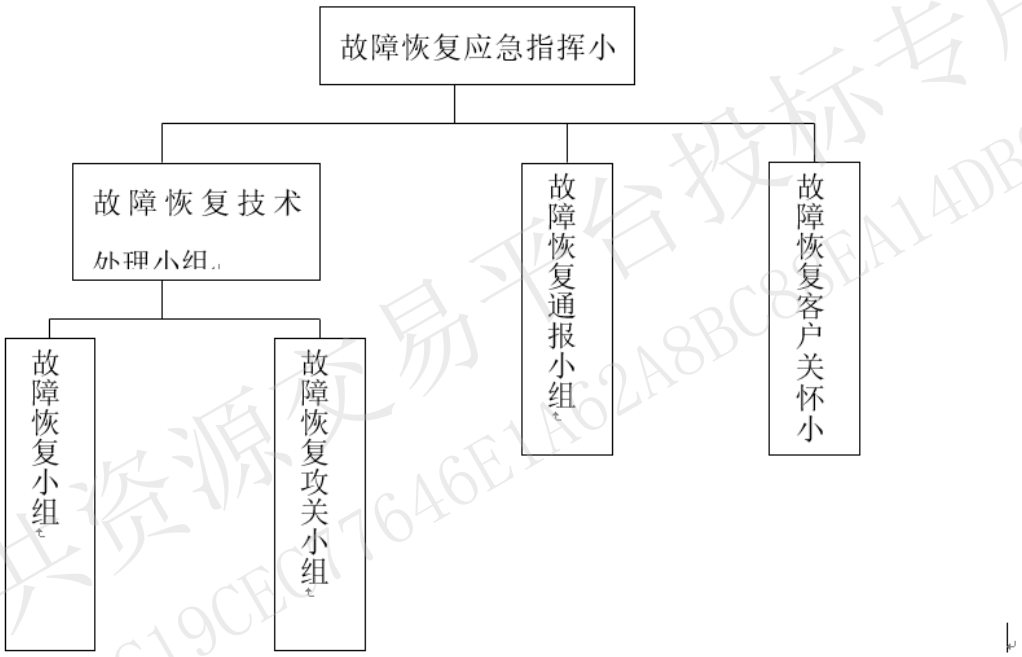
（6）资源备份及快速恢复

发生业务数据损坏时，维护人员应及时报告应急领导小组，检查、备份业务系统当前数据。

维护人员应待业务数据系统恢复后，检查历史数据和当前数据的差别，由相关系统业务员补录数据；重新备份数据，并写出故障分析报告，在调查工作结束后一日内报告应急领导小组。

环境正常以后，将硬件设备恢复到原来状态，若数据有错误，利用最近日期的数据备份磁带进行恢复。

3.6.2 应急组织架构



故障恢复应急小组指挥小组：由华为技术有限公司安排的客户服务经理和客户方的维护主管组成，负责整个应急处理的资源调度、应急恢复的有效组织和管理。

故障恢复技术处理小组：有华为技术有限公司的区域服务支持工程师、总部技术支持专家及研发组织，负责故障的技术公关、故障恢复方案的制定以及故障恢复方案的实施等。

故障恢复通报小组：由华为技术有限公司区域技术支持工程师、热线响应中心、服务代表等组成，负责及时通报问题的处理最新进展。

故障恢复客户关怀小组：由华为技术有限公司区域市场代表、区域服务代表

公共资源交易平台投标专用

等组成，负责故障发生时、故障处理过程中、故障恢复后客户沟通和安抚。

3.6.3 响应时间

节假日以及重要时间节点运维团队人员驻守机房进行 7*24 现场保障，保障包括但不限于平台运行和信息安全，同时保障人员进行 7*24 小时电话响应。重保期间，运维部门针对重大节点进行 7*24 小时实时监测平台的网络、存储、计算等设备运行情况，做到及时检修、及时发现故障、及时汇报，遇到重大故障按照上报流程及时向上级报告，及时排除故障，确保平台整体可用性。

3.6.4 电力应急

为了保障政务云机房和综合楼生产用电安全，一旦电源出现故障，能及时处理和尽快恢复正常供电，特制定本预案。

应急预案启动条件:

本预案适用于政务云机房生产电力保障，在突然出现局部停电或高压供电设备发生故障时，可立即启动本预案。

应急预案执行原则:

当出现局部停电或供电设备故障时，单位配备的发电机组立即启动进行供电，首先保证政务云机房用电，保证政务云生产机房用电安全，确保政务云服务与厅局业务正常运行。

预案保障措施:

1、 按照工作计划对电源设备、蓄电池、UPS 等配套电源设备进行检查和维护，排除存在的故障隐患，始终保持电机、蓄电池容量正常和完好。

2、 坚持保养维护制度，开展日常演练，熟悉油机启动和停送电的模拟供电，保证每个人都能掌握油机启动步骤和停送电步骤。

3、 按照规定每月对发电机组进行开机试运行，确保油机在紧急情况下 10 分钟内可以正常启动进行供电。

4、 与电力部门保持联系，了解市电停电情况，确认停电性质和估测停、来电时间，及时对油机燃料等进行相应调整。

5、 电力值班人员对重点部位增加巡检次数，确定每个设备厂家的售后维修联系方式，出现不能解决的故障及时与厂家技术人员联系，寻求支持。

公共资源交易平台技标专用

3.6.5 空调应急

当机房空调系统发生故障，需要尽快对故障进行排除时，应启用机房空调故障应急预案。

预案启动条件

机房空调系统发生不制冷、漏水等故障，影响到环境温度控制时，启动本预案。

应急处置步骤

1、发现室温过高，进而发现空调系统发生故障。并向上级主管领导汇报空调设备故障情况。

2、检查是否因为电力中断导致的设备停机，注意检查线路接触不良、保险丝烧断等情况，当发现电力中断时，需要及时联系供电部门进行抢修。

3、检查设备的配置情况，注意分辨是否因为如下原因导致的空调运转不良：预设定室温温度过高、空调启用了定时功能、设备短路保护导致自动停机。

4、联系空调维修人员前来进行故障排除。尽可能要求维修人员采用现场备件更换的方式，迅速修复设备故障。

5、当空调设备不能使用时，需要考虑变通的降温措施来控制机房温度上升，措施有：

安放电风扇对机房进行通风换气降温，对重要设备考虑放置单独风扇进行降温；

开启机柜的风扇开关，增加机柜换气速度，全封闭机柜可考虑开门开挡板增加换气量；

考虑关闭临时设备，降低机房设备整体发热量；

必要时在机房放置冰块，实现迅速降温的目的。

6、设备恢复正常后，向主管领导汇报本次事件处理情况并文件归档。

应急处置完成

机房空调系统经过重新配置工作恢复正常，或经过厂商检修后恢复正常使用。

事件级别判定

业务时间恢复时间低于 10 分钟超过 5 分钟、非业务时间低于 24 小时超过 8 小时的，属于 III 级事件。

公共资源交易平台投标专用

业务时间恢复时间低于 30 分钟超过 10 分钟、非业务时间低于 48 小时超过 24 小时的，属于 II 级事件。

业务时间预计或实际恢复时超过 30 分钟、非业务时间超过 48 小时的，属于 I 级事件。

预案演练要求

1）可有选择的挑选部分设备进行演练操作。

2）准备空调维修人员的联系方式

3）熟悉空调电源位置和空调操作方法。

4）演练结束形成演练总结报告。

应急准备措施

应急处置人员需要具备必要的空调设备操作技能，并且配备电工工具、备用风扇、盛冰容器等。

3.6.6 消防应急

当机房发生火灾时，需要进行人员撤离与消防操作时，应启用机房火灾消防应急预案。

预案启动条件

机房发生火灾时，启用本预案。

处置步骤

1、发现火灾并确认满足预案启动条件，启动此预案流程；

2、通知周围同事和大楼保安机房发生火灾；

3、通知大楼电力部门切断机房电源；

4、通过手机、固定电话或短信等方式向主管领导报告机房火灾；

5、主管领导同意或 2 分钟内无法得到主管领导意见，且根据火势情况需要报警的情况下，拨打 119 报警，报告内容为：“XX 单位机房发生火灾，请迅速前来扑救。地址 XXX”，待对方放下电话后再挂机；

6、安排人员等待并指引消防人员；

7、根据火势情况采取措施疏散人员或组织紧急扑救；

8、组织人员配合消防人员实施扑救；

9、防火安全检查及事故分析；

公共资源交易平台投标专用
AE2C15CE27646E1A62A8BC88D14DB9

10、恢复受损系统；

11、调整防火设备和检查防火管理制度；

12、损失评估；

13、安全报告、归档；

14、形成事故分析报告，分析事故原因，修正应急预案的处理流程并归档。

应急处置完成

1）火灾及其隐患全部消除；

2）人员妥善安置并且机房恢复正常业务。

3.6.7 网络及系统应急

针对网络及系统出现的问题，制定基于场景化的应急预案，保障网络及系统出现问题后能尽快恢复，保证业务的稳定运行。在重大事件前，对网络架构、资源负荷进行评估，并根据实际情况给出适当的优化建议和改进措施。

预案保障措施

在重大节假日/关键事件保障期间，原厂派保障工程师到（指定的）现场提供值守保障支持。对网络/业务系统运行状态进行分析，及时发现问题，评估风险，提前预警；在发生故障时提供最快的现场响应和支持，协助集团实施应急预案，尽快排除故障，保证网络稳定运行。服务内容如下：

实时告警监控

安排工程师在网管中心实时监控故障告警，及时发现问题，评估风险，提前预警。

实时问题处理

安排工程师在网管中心，现场进行问题处理，故障恢复服务，及时传递前后方信息，处理各种突发问题。

实时 KPI 性能监控

安排工程师在网管中心实时监控网络性能状态，及时发现指标恶化趋势，提前预警。

实时参数优化

安排工程师在网管中心针对恶化的 KPI，及时进行参数调整，优化

远程专家值守

公共资源交易平台技术专用

安排研发专家在远程进行值守，针对重大问题立即介入，确保问题快速解决

现场应急支持

工程师在网管中心或机房（设备）现场，提供现场技术支持或者故障恢复服务，及时传递前后方信息、现场调整和实施应急预案、处理各种突发问题、提出专业合理建议。

网络评估

对网络架构、资源负荷进行评估，并根据实际情况给出适当的优化建议和改进措施。

报告服务

根据要求，定期发送网络及业务系统的运行报告。

提交服务总结报告

提供服务总结报告，并提出合理建议。

3.6.8 云平台故障应急

云平台是用于生产系统运作的基础平台，主要为业务系统提供计算资源、网络资源、存储资源。系统需要 24 小时不间断地运行，系统重要程度高。

云平台重大故障点主要来源于以下 4 个方面：

1. 计算节点服务器主机硬件故障；

2. 两台接入交换机同时故障；

3. 存储设备故障；

4. 管理节点物理服务器主机硬件故障；

云平台故障应急预案需要从这 4 个方面指导和规范故障时技术操作和信息报送，确保在合理的时间内恢复系统正常运行，达到风险可控的目的。

场景	场景描述	事件等级	故障现象
场景一	计算节点服务器主机硬件故障	紧急	故障现象：主机主要硬件故障（例如主板、RAID 卡等）、突然断电等。 影响范围：该主机上的虚拟机运行闪断。触发主机 HA 后，在资源允许情况下，会在正常的主机上重建虚拟机

公共资源交易平台投标专用

场景二	两台业务接入交换机同时故障	紧急	故障现象：大批量的业务虚拟机无法登录 影响范围：大量业务系统无法使用
场景三	存储设备故障	紧急	故障描述：服务器网卡/HBA 故障、IP 存储/FC 交换机故障/SmartI/O/存储控制器故障等。 影响范围：可能影响虚拟机的正常运行，业务系统可能不可用，前端用户可能访问不了。
场景四	管理节点物理服务器主机硬件故障	高	故障现象:Openstack 的控制节点操作系统无法启动。 影响范围：不影响虚拟机运行，不影响业务系统，管理平台中断 10 分钟左右。

处理流程

云平台运维人员发现故障后，直接向华为技术有限公司技术支持热线 4008229999 进行故障申告。

云平台运维人员配合 400 支持工程师提供产品故障现象和相关信息收集，400 工程师确定故障原因，400 工程师确定硬件故障需要现场服务时，马上派单给片区工程师，由工程师申请备件，前往现场进行故障处理。要求确定故障原因时间在获得完整的产品故障现象和相关信息后 30 分钟以内，现场工程师在 30 分钟内得到备件并且准备出发。

针对用户的常规配置问题，400 支持工程师协助客户进行故障排除。80%软件问题可以被解决掉。

如果系统发生软件故障，并且无法确定故障原因和恢复方法时，确认需要现场工程师服务时，马上安排相关工程师现场服务，并且升级故障为疑难故障。现场工程师在规定时间达到现场。同时 400 技术支持中心组建专家团，对故障进行先期分析。由现场工程师收集更详细的资料提供到专家团队进行分析，由专家团进行故障定位和给出处理方案，由一线工程师按照方案进行故障处理。本阶段基

公共资源交易平台投标专用

本可以处理 15%左右的故障。

400 专家团在 1 小时内无法解决故障，通报后台研发人员，研发团队做好故障处理的准备工作。2 小时还无法解决问题，上升到产品研发团队，并且升级问题级别为高级疑难问题，由研发团队进行故障分析和处理。研发团队负责完成剩余 5%的故障。

3.6.9 应急演练

安全应急演练服务是模拟南阳政务云平台及应用出现网络安全事件时，根据事前制定的应急预案、组织相关各方（包括南阳市政府监管部门、政务云各局委办租户、云服务商）协同配合，参与安全应急演练，并在事后针对应急演练情况，进行总结，发现演练中存在的不足，形成报告，提交给政府监管部门、局委办和云服务商。

我方每年组织进行 2 次应急演练，工作内容包括制定安全应急方案、参与演练、协助总结梳理，形成演练总结报告。

安全应急演练主要包括：制定应急演练预案及演练计划、执行安全应急演练，以及演练回顾三个阶段。

- **制定应急演练预案及演练计划**

由云服务提供商组织监管部门、局委办代表，参考政务云资产清单，明确安全应急演练目标。云服务提供商制定应急演练计划，要求演练计划符合南阳市政府相关的管理要求，并且和涉及的局委办租户沟通达成一致。接下来针对目标系统，制定安全应急演练方案。方案中将包括：演练内容与范围、演练目的、演练时间安排、故障场景、处置流程与技术方案。

应急演练方案需要经过安全专家、云服务提供商、局委办租户评审通过后方可执行。

- **执行安全应急演练**

按照既定的演练计划，组织相关各方进行安全应急演练。成立安全应急演练指挥小组，负责指挥计安全应急预案的落实情况、协调参与部门、处理突发事故、监督应急演练顺利进行。由涉及的局委办租户、云服务提供商协同按照应急预案的内容，进行应急演练。

- **演练总结**

公共资源交易平台投标专用

演练结束后，云服务提供商对演练活动进行总结。同时根据实际情况，对应急演练预案、演练流程进行相应优化。

本阶段输出文档：

《南阳政务云 XX 系统安全应急演练方案》

《南阳政务云 XX 系统安全应急演练验证方案》

《南阳政务云 XX 系统安全应急演练计划》

《南阳政务云 XX 系统安全应急演练总结报告》

3.7 信息安全保障服务方案

我方能遵循国家电子政务信息安全保障体系要求，参考国家主管部门发布的相关标准规范要求，提供明确、完善、可行的安全建设方案，充分考虑在网络、系统、数据库、应用等方面的安全性。

我方须从机房、网络、安全、虚拟机、物理机、存储、运维等方面加强信息安全管理，避免因出现问题引起信息安全责任事故。

信息安全保障服务方案应从保障措施、预防措施、风险评估、质量保障等方面来阐述说明。

3.7.1 信息安全保障内容

机房应该设置物理层安全措施，如门禁、摄像头等。每一个机柜应该配备锁定设备，确保机柜内的设备不会被未授权人员访问和移动。此外，还应该定期检查物理层设备的状态，如电缆连接、接头、风扇等。机房管理人员应该定期检查设备的状态，如服务器、交换机、路由器等。如果发现硬件故障或其他问题，应及时检查和修复。机房应实现 7*24 小时的监控和值守，保证机房的安全稳定运行，实时监控运行状态，且专门配属具备多年大型 IDC 维护经验，资深电力、空调等动力设施维护支持人员和资深网络等基础设施运维人员。

网络信息安全是指网络中传输和保存的数据，不受偶然或恶意的破坏、更改和泄露，网络系统能够正常运行，网络服务不中断。保障网络信息安全，应从密码技术、防火墙、入侵检测技术、访问控制技术、虚拟专用网技术、认证技术等来进行防护。

物理机应及时安装系统补丁，任何操作系统都有漏洞，及时打上补丁避免漏

公共资源交易平台投标专用

洞被蓄意攻击利用，是服务器安全重要的保证之一。物理机安装和设置防火墙，对服务器安全而言，安装防火墙非常必要。防火墙对于非法访问具有很好的预防作用，但是安装了防火墙并不等于服务器安全了。在安装防火墙之后，还需要根据自身的网络环境，对防火墙进行适当的配置以达到最好的防护效果。物理机上安装杀毒软件。现在网络上的病毒非常猖獗，这就需要在网络服务器上安装网络版的杀毒软件来控制病毒传播。同时，在网络杀毒软件的使用中，要定期或及时升级杀毒软件，并且每天自动更新病毒库。定期对物理服务器进行备份。为防止不能预料的系统故障或用户不小心的非法操作，必须对系统进行安全备份。服务武器上的账号和密码保护可以说是服务器系统的第一道防线，目前网上大部分对服务器系统的攻击都是从截获或猜测密码开始的。一旦黑客进入了系统，那么前面的防卫措施几乎就失去了作用，所以对服务器系统管理员的账号和密码进行管理是保证系统安全非常重要的措施。

存储系统作为数据的保存空间，是数据保护的最后一道防线；首先是加密，以防被非法窃取，造成不必要的损失。其次，可以定期备份加密后的重要数据，云存储环境采取分布式方案，使得数据的安全性有充足的保障。

运维在信息安全保障诸要素中，人是最关键也是最活跃的要素。对所有员工，进行信息安全保障意识教育，诸如采取内部培训、在组织机构网站上发布相关信息等方式，增强所有员工的安全意识；对信息系统应用岗位的员工，进行信息安全保障基本技能培训；对信息安全专业人员，应通过对信息安全保障、管理、技术、工程，以及信息安全法规、政策与标准等知识的学习，全面掌握信息安全的基本理论、技术和方法，丰富的信息安全经验需要通过该岗位的长期工作积累获得；信息安全研发人员，除了需要具备信息安全基本技能外，还应培训其安全研发相关知识，包括软件安全需求分析、安全设计原则、安全编码、安全测试等内容；信息安全审计人员，则需要通过培训使其掌握信息安全审计方法、信息安全审计的规划与组织、信息安全审计实务等内容。

3.7.2 保障措施

信息安全保障就是针对信息系统在运行环境中所面临的各种风险，制定信息安全保障策略，在策略指导下，设计并实现信息安全保障架构或模型，采取技术、管理等安全保障措施，将风险控制到可接受的范围和程度，从而实现其业务使命。

因此所有维护和管理人员应增强保密观念，熟悉并严格执行保密规定，各级领导必须经常对维护人员进行保密教育，内部定期组织检查，发现问题及时整改。具体包括：

（1）建立健全网络与信息安全规章制度，以及各项规章制度执行情况监督检查；

（2）开展网络与信息安全风险监测预警和评估控制、隐患排查整改工作；

（3）建立健全网络与信息安全事件应急处置和上报制度，以及组织开展应急演练；

（4）建立健全从业人员网络与信息安全教育培训以及考核制度；

（5）违法有害信息监测处置

3.7.3 预防措施

安全控制措施的目的之一是防止发生信息安全事件，但由于信息系统内部固有的脆弱性和外在的各种威胁，很难彻底杜绝信息安全事件的发生。所以，应及时有效地响应与处理信息安全事件，尽可能降低事件损失，避免事件升级，确保在组织能够承受的时间范围内恢复信息系统和业务的运营。

为了预防信息泄露事件的发生，为发生安全事件后能够采用有效的办法和良好的沟通、协调流程处理安全事件，应当制定一些预防的措施，以确保安全事件的及时响应工作，具体包括：

1）为保障用户权益，机房人员不得利用工作之便擅自跟踪、窃听用户通信。

2）各种保密信息未经允许不准擅自携带外出，不得以任何方式泄露给任何人。

3）确需提供相关数据或资料的，由相关管理人员负责审核手续是否完备，经授权审批后方可整理相关数据和资料并提供。

4）保密信息使用人、保管人对保管的信息进行定期清理，对已作废的、或者已无权再接触的文件要删除或销毁。

5）除非信息所有人批准，否则员工不能保留与当前岗位无关的保密信息。当员工离开原岗位（含离职）并工作交接完毕后，应该删除或销毁所有与原岗位相关的保密信息。

6）删除或销毁存档性质的保密信息，以及集中批量删除或销毁保密信息必须

公共资源交易平台投标专用

由相应级别主管批准，并按相应的管理规定处理。

7）含保密信息的纸件必须用碎纸机销毁，而不能直接扔垃圾箱或用手撕毁。含秘密级以上信息的纸件不能重复使用。

8）在拷贝过程中，废弃的保密信息必须销毁，例如：复印效果不好的纸件、打印未完成的纸件等。

9）含保密信息电子件的存储介质作废时应采取不能恢复的物理性销毁。

3.7.4 风险评估

信息：信息是一种资产，具有价值，需要进行恰当的保护，如果泄露，可能会用户造成损失和不良影响。信息可能以很多形式存在，如：纸件、电子件。信息的传输也可能是很多形式，如：交谈、电话、电子邮件、传真等。

保密信息：保密信息是指对用户具有重要价值或敏感的信息，不能公开发布，需要进行恰当的保护，如果泄露，可能会给用户造成损失和不良影响。保密信息包括但不限于：商业秘密包括技术秘密和经营秘密，其中技术秘密包括但不限于工作进度、技术方案、工程设计、电路设计、制造方法、配方、工艺流程、技术指标、计算机软件、数据库、研究开发记录、技术报告、测试报告、检测报告、实验数据、试验结果、操作手册、技术文档、相关的函电等。经营秘密包括但不限于客户名单、行销计划、采购资料、定价政策、财务资料、进货渠道、法律事务信息、人力资源信息等。

信息安全风险产生的因素主要有信息系统自身存在的漏洞和来自系统外部的威胁。信息系统运行环境中存在具有特定威胁动机的威胁源，通过使用各种攻击方法，利用信息系统的各种脆弱性，对信息系统造成一定的不良影响，由此引发信息安全问题和事件。

信息安全管理就是依据安全标准和安全需求，对信息、信息载体和信息环境进行安全管理以达到安全目标。风险管理贯穿于整个信息系统生命周期，包括背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询 6 个方面的内容。其中，背景建立、风险评估、风险处理和批准监督是信息安全风险管理的 4 个基本步骤，监控审查和沟通咨询则贯穿于这 4 个基本步骤的始终。

3.7.5 质量保障

为确保信息安全，要坚持积极防御，综合防范的方针，全面提高信息安全防

护能力。建设信息安全管理体系，建立完善的安全管理制度，将信息安全管理，自始至终贯彻落实于信息管理系统的方方面面，信息安全才能得以实现。信息安全的解决方案。信息质量保障包括：

1、对应用系统使用、产生的介质或数据按其重要性进行分类,对存放有重要数据的介质(盘、移动存储设备),必须进行备份,并分别存放在不同的安全地方(防火、防高温、防震、 防磁、防静电及防盗),建立严格的保密保管制度。

2、保留在机房内的重要数据,应为系统有效运行所必需的最少数量即一套,除此之外禁止留在机房内。

3、根据数据的保密规定和用途,确定使用人员的存取权限、存取方式和审批手续,并设定 同级别的登陆密码。

4、重要数据(介质)库,设专人负责登记保管,未经批准,不得随意挪用重要数据(介质)。

5、在使用重要数据(介质)期间,严格按保密规定控制转借或复制,需要使用或复制的须经 准,并做好保密备份登记。

6、对所有重要数据(介质)定期检查,考虑介质的安全保存期限,及时更新复制。损坏、废， 或过时的重要数据(介质)由专人负责处理,秘密级以上的重要数据(介质)在过保密期或废弃不月 时,及时销毁。

7、机密数据处理作业结束时,及时清除存储器、硬盘及其它介质上有关作业的程序和数据。

8、机密级及以上秘密信息存储设备不得并入互联网。

9、重要数据不得外泄,重要数据的输入及修改由专人来完成;重要数据的打印输出及外存 质应存放在安全的地方,打印出的废纸及时销毁。

为确保 IDC 机房的安全可靠，建立有效的安全机制，现场值班人员通过门禁系统控制对 IDC 机房的访问，非授权人员不得进入。IDC 机房配备全球眼监控系统、对机房实行 7*24 小时的实时监控。

对机房内所有物品实行严格的事前进出审批及进出登记制度，对记录文档妥善保留一年。对授权进入机房内的服务厂商，全程陪同并作记录。

公共资源交易平台投标专用

3.8 信息安全保障服务能力

3.8.1 基本安全服务

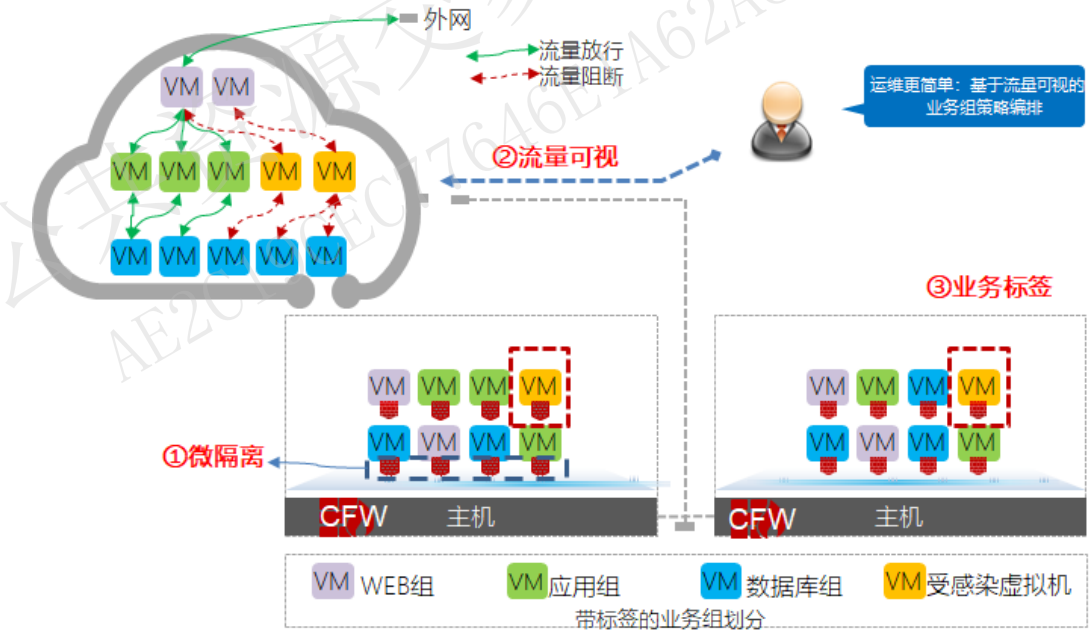
3.8.1.1 虚拟防火墙

云防火墙（Cloud Firewall）为租户 VM 提供微隔离能力，并通过流量可视化、基于业务属性标签的安全策略配置手段来降低安全运维复杂度。云防火墙服务依赖分布式的 iptables 相关能力实现。

功能特点：

- 微隔离：提供 VM 到 VM 级细粒度的访问规则配置能力
- 流量可视：基于拓扑图访问关系辅助用户定义策略
- 业务标签：基于业务标签进行防护对象定义

安全管理员可以使用云防火墙，为业务提供基于 VM 粒度的安全防护，基于业务标签来定义安全策略，使用流量可视功能辅助策略配置，从而实现简化运维复杂度，提升防护效果。



3.8.1.2 虚拟漏洞扫描

漏洞扫描服务主要适用于以下场景：

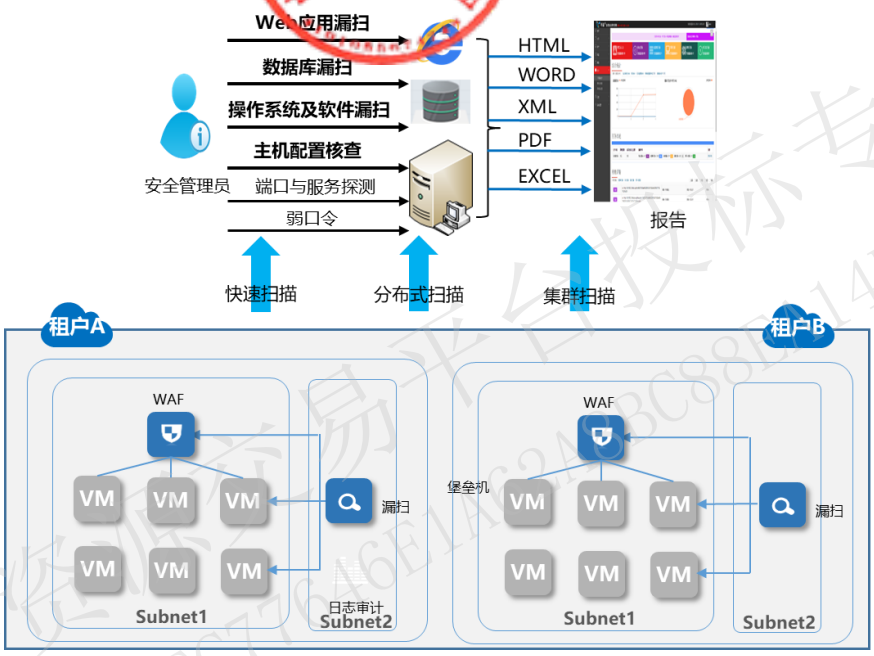
（1）综合漏洞探测和弱口令检查：

支撑 Web 应用弱点扫描、数据库弱点扫描、系统弱点扫描、应用软件安全检测，弱口令、端口与服务探测等综合漏洞探测。

支持对 FTP、TELNET、POP3、SMB、SSH、ORACLE、SMTP、IMAP、Mysql、MSSQL、DB2、、REDIS、RLOGIN、RDP、RTSP 等协议的弱口令检查。

（2）提供综合风险评估报告及漏洞修复建议

提供对租户资产的风险评估报告，对每个漏洞提供涉及受影响资产、漏洞等级、CVSS 评分、漏洞的详细描述，以及针对该漏洞的修复建议。租户用户可以基于报告的修复建议进行系统加固。



云漏洞扫描流程图

漏洞扫描服务提供如下功能：

漏扫支持能力

Web、数据库、基线核查、操作系统及应用软件、弱口令、端口探测与服务识别 5 大扫描功能

分布式集群

分布式集群管理模块：漏洞扫描服务集成了 Web 扫描、系统扫描、基线核查、数据库扫描等，转化成 B/S 扫描框架，扫描更稳定、更快速、更易于扩展。除此之外，为了更大程度上实现快速扫描、分布式扫描，和以数百上千网站为目标的集群扫描，突破原本单机扫描器难以实现的批量扫描、集团网扫描障碍，在集成原引擎的前提下，实现了分布式集群管理模块，实现各

引擎节点间任务的自由流转，高度智能分配资源，提高资源利用率

综合报表

统计报告内容同样支持用户自定义，极大程度上丰富了可用性与易用性。并且支持主流报告格式，包括：HTML、XML、PDF、WORD、EXCEL 五大报告格式。高度可视化的统计结果以及多维度的统计对比数据，标准的报告文档，让用户可以直观的看到自己的系统状态，报告文件告别人工修订

基线核查

安全配置核查系统帮助用户对云平台中租户资产的虚拟服务、物理服务器、网站中间件的配置文件进行自动化的检查，及时发现其中的安全威胁，并及时告知用户进行修正。

安全配置核查系统支持对 Windows 系列、Linux 系列、Unix 等操作系统进行安全基线检查；支持对 Tomcat，IIS，WebSphere，Apache，BIND 等中间件进行安全基线检查

3.8.1.3 **虚拟堡垒机**

云堡垒机（Cloud Bastion Host，CBH）是华为云 Stack 的一款 4A 统一安全管控平台，为企业提供集中的帐号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。云堡垒机提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。

公共资源交易平台投标专用



云堡垒机流程图

账户管理：集中管理系统用户和资源帐号信息，对帐号全生命周期建立可视、可控、可管运维体系。

权限控制：集中管控用户访问系统和资源的权限，对系统和资源的访问权限进行细粒度设置，保障了系统管理安全和资源运维安全。

操作审计：基于用户身份系统唯一标识，从用户登录系统开始，全程记录用户在系统的操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。包括：

- Web浏览器运维
- 第三方客户端运维
- 自动化运维

高效运维：通过多种架构运维、多种运维资源、多种运维工具、多种运维形式的接入，全面提升运维效率。

3.8.1.4 虚拟主机安全

企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

公共资源交易平台投标专用

企业主机安全服务（HSS）主要适用于以下场景：

- 等保必备：满足入侵检测、恶意代码防范、漏洞检测等条款
- 病毒防御：有效检测查杀勒索、挖矿、后门等恶意程序
- 主机加固：检测主机漏洞、弱密码等，根据结果进行加固
- 入侵检测：检测黑客入侵行为，应对高级威胁、红蓝对抗
- 安全运营：自定义安全策略积累固化安全团队实战经验；提供安全总览用于安全工作汇报，周边团队交流



云主机安全防护流程

主机安全功能特性：

功能项	功能描述
资产管理	资产管理功能可深度扫描出主机中的账号、端口、进程、软件信息和自启动任务等。
漏洞管理	漏洞管理功能将检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞，帮助用户识别潜在风险。
入侵检测	入侵检测功能可识别并阻止入侵主机的行为，实时检测主机内部的风险异变，检测并查杀主机中的恶意程序，识别主机中的网站后门等。

功能项	功能描述
基线检查	基线检查功能可扫描出主机系统和关键软件含有风险的配置信息。

表 0-10 主机安全特性

3.8.1.5 虚拟Web应用防火墙

Web 应用防火墙（云 WAF）服务主要应用于以下场景：

（1）防止数据泄漏

防止恶意访问者通过注入式攻击、网页木马、WebShell 等攻击手段入侵网站，窃取重要商业机密或敏感信息等，保护网站远离信息泄露风险；

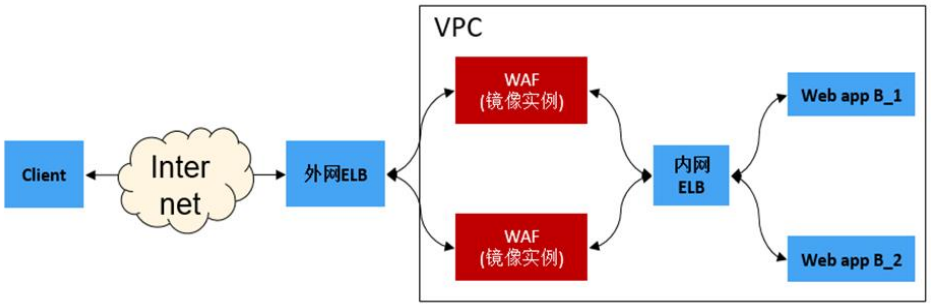
（2）抵御 CC 攻击

当网站遭受 CC 攻击时，大量恶意请求长时间占用网站计算资源，导致网站业务响应缓慢甚至无法提供正常的服务，Web 应用防火墙可以精准识别 CC 攻击并过滤恶意请求，使普通用户能正常访问网站提供的业务；

（3）保护网站访客安全

Web 应用防火墙能识别跨站脚本（XSS）、网页木马、跨站请求伪造（CSRF）等攻击行为，除了保护自身安全以外，还能保护网站访问者的安全，避免信息泄露引起的纠纷和负面影响。





云WAF防护流程

功能特性如下：

功能项	功能描述
引擎实例管理	提供引擎实例订购与删除能力
防护网站管理	提供防护网站的创建、查询、修改和删除能力
防护策略管理	提供防护策略的创建、查询、修改和删除能力
事件查看	提供安全总览、详细事件日志查看、事件告警通知能力
Web防护	提供Web流量检测与攻击拦截的防护功能
运维告警	提供组件状态检查，资源告警的能力

WAF功能特性

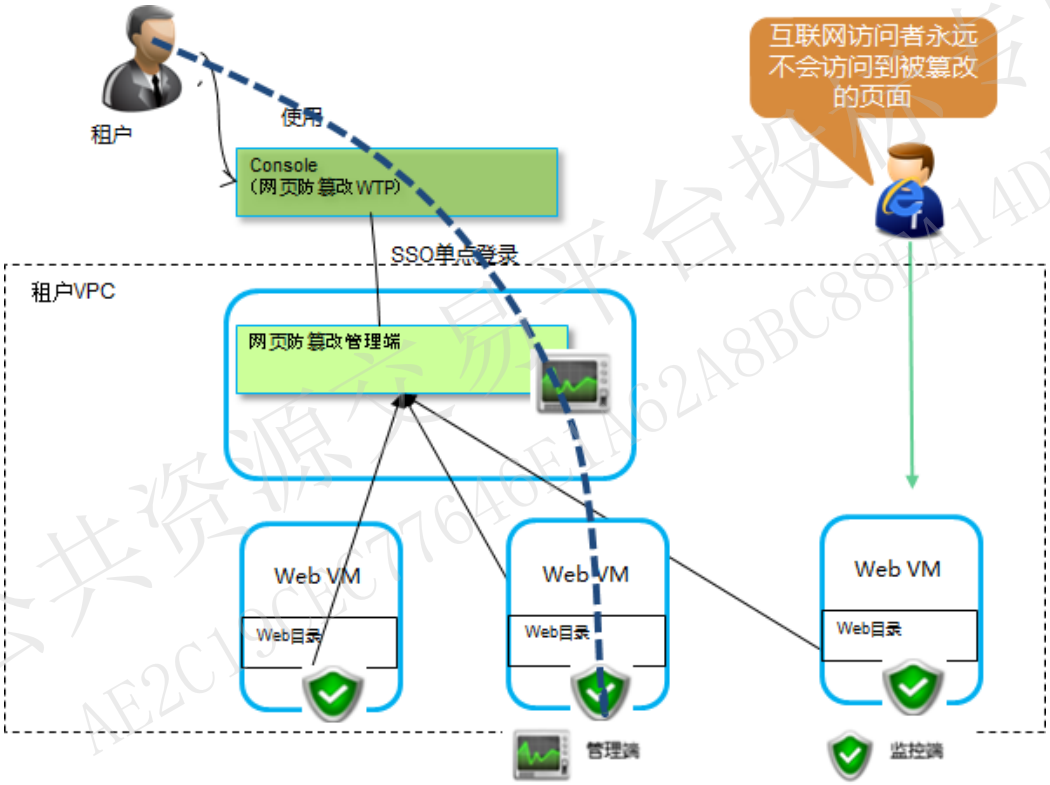
3.8.1.6 网页防篡改

网页防篡改服务从系统底层驱动实现多种保护模式，防止静态和动态网站内容被非法篡改，保证网站内容的正确性。

网页防篡改服务提供如下功能：

- 网页文件保护：通过 web 防攻击模块、防篡改模块（系统内核层的文件驱动），可对动态和静态网页文件进行完美的保护。按照用户配置的进程及路径访问规则，设置网站目录、文件的读写权限，限制文件目录的增、删、改操作行为，确保网页文件不被非法篡改。
- 集中管理：通过监控端集中管理多台 Web 服务器，监测多主机实时状态，制定保护规则，接收 Web 服务器的报警和日志信息。控制 Web 服务器的启用、关闭、禁用等状态，并可对 Web 服务器的日志和报警情况做统计分析。
- 实时报警：对非法篡改行为，系统会自动记录报警日志，并通过手机短信、电子邮件、syslog 等多种方式通知管理员。能对网站攻击做到快速响应，及时应变。
- 管理员权限分级：可对管理员及监控端分配不同的权限组合。
- 日志审计：提供管理员行为日志，包括：时间、事件、操作对象、行为、IP 地址等详尽信息，方便区分正常更新过程还是篡改攻击行为；支持保护日志查询审计功能；用户不能进行日志修改、删除操作，确保日志的准确性与完整性。

- 站点文件保持：防篡改模块集成在 Web 服务器软件中，通过设定各种站点文件访问过滤规则，对多个站点文件或单个站点的文件夹进行保护。
- 系统信息检测：管理控制端机器能记录所有监控端 Web 服务器的 CPU、内存、硬盘等应用情况，方便管理员根据提供的硬件信息做升级和维护调整。
- 系统自我保护：网页防篡改系统能够实时地保护自己，不被非法的删除、修改、卸载等，保证了即使服务器被非法入侵，也不能够对网站进行篡改，不能够对网站管理系统进行破坏。

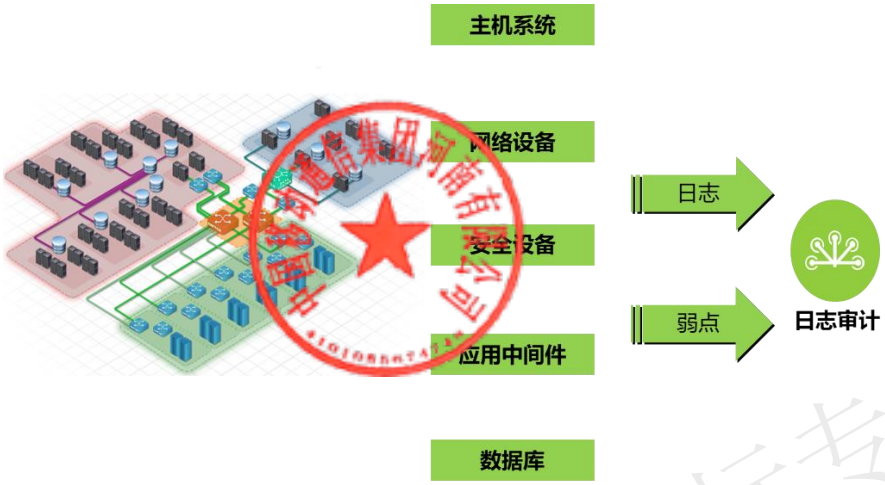


租户申请网页防篡改服务后，会在租户的业务网络拉起承载防篡改管理端的虚拟机，即防篡改安全实例。在防篡改管理端下载相应的防护客户端，部署在需要防护的 Web 服务器上，配置需要防护的 WEB 目录。在正常使用时，可以通过登录网页防篡改服务，通过单点登录的模式掉转到网页防篡改的客户端，配置使用。

3.8.1.7 虚拟日志审计

日志审计服务是信息系统的综合管理平台，通过对租户 ECS 主机、业务应用

以及第三方在镜像市场上线的各种业务系统的日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保客户业务的不间断运营。



云日志审计流程图

日志审计的主要功能如下：

全面日志采集

实现云上信息资产的日志获取，并通过预置的解析规则实现日志的解析、过滤及聚合。

智能关联分析

实现全维度、跨设备、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，客户可轻松实现各资产间的关联分析。

脆弱性管理

能够收集和管理来自各种 Web 漏洞扫描、主机漏洞扫描工具、网络漏洞扫描工具的产生的扫描结果，并实时和用户资产收到的攻击危险进行风险三维关联分析。

数据挖掘和数据预测

支持对历史日志数据进行数据挖掘分析，发现日志和事件间的潜在关联关系，并对挖掘结果进行可视化展示。系统自带多种数据统计预测算法，可以根据历史数据的规律对未来的数据发生情况进行有效预测。

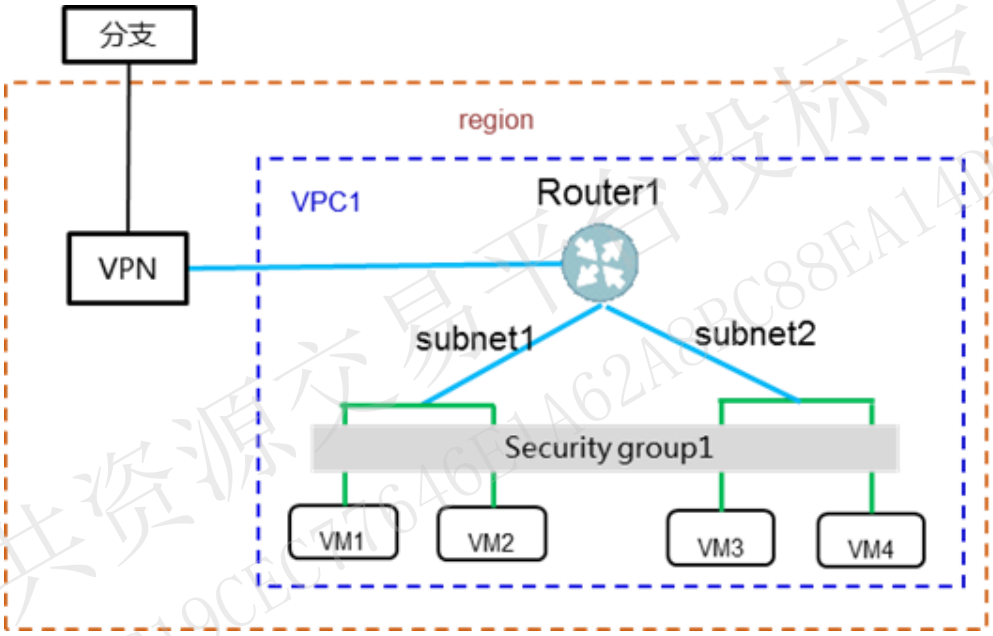
可视化展示

公共资源交易平台投标专用

实现所监控的信息资产的实时监控、信息资产与客户管理、解析规则与关联规则的定义与分发、日志信息的统计与报表、海量日志的存储与快速检索以及平台的管理。通过各种事件的归一化处理，实现高性能的海量事件存储和检索优化功能，提供高速的事件检索能力、事后的合规性统计分析处理，可对数据进行二次挖掘分析。

3.8.1.8 虚拟VPN接入

虚拟 VPN 用于租户业务安全接入，VPN（Virtual Private Network）即虚拟专用网络，用于分支机构和 VPC 之间建立一条安全加密的通信隧道，把企业已有数据中心和云上的网络打通。



VPN业务流程

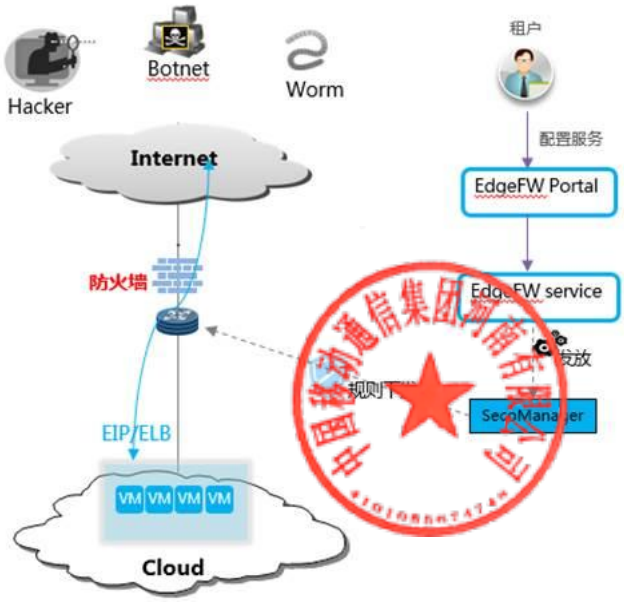
本项目提供 IPSec VPN 以及 SSL VPN 能力。

3.8.1.9 虚拟防病毒

边界防火墙服务主要适用于以下场景：

云数据中心与外部网络之间的南北向流量，为用户提供边界安全防护功能，帮助用户进行实时的云上边界安全高级防护，支持入侵防御和防病毒。

公共资源交易平台投标专用



边界防火墙服务（Edge Firewall Service）针对云数据中心与外部网络之间的南北向流量，为用户提供边界安全防护功能，支持以弹性公网IP为防护对象的入侵检测防御（IPS）和网络防病毒（AV）功能。

边界防火墙服务的主要功能如下：

- 安全防护：可针对弹性公网 IP（EIP/ELB）进行南北向流量的访问控制、入侵防御和防病毒；
- 安全日志：根据源、目的地址、日期、攻击类型、协议等查看日志明细；
- 统计报表：图表的形式展示攻击类型、趋势、协议等排行。

3.8.1.10 入侵检测

网络检测与响应（Network Detection and Response，简称 NDR）是基于华为多年攻防经验，运用特征规则、大数据分析等技术，对企业网络流量进行实时检测、捕获、解码、审计，发现企业网络和系统中存在的安全风险和威胁，实现四到七层网络流量防护的安全平台。

公共资源交易平台投标专用

当主机遇到常见 Web 攻击时，NDR 通过分析 7 层协议（包括 HTTP/Redis/MySQL 等交互协议），对流经核心路由器的流量进行全量检测。当检测到一些恶意特征的流量时，NDR 通过构造阻断包，经核心路由器转发给攻击者和主机，从而阻断访问，为平台的主机提供安全防护，其主要架构如下图所示。



NDR 的阻断原理如下：

5. 攻击者的流量流入核心路由器，再由核心路由器转发给主机。
6. 同时，核心路由器的流量经分光器拷贝到 NDR。
7. NDR 通过检测确认为网络攻击后，发送构造的阻断包给核心路由器。
8. 核心路由器将构造的阻断包分别转发给攻击者和主机从而阻断攻击访问。

NDR 主要有以下功能：

- 攻击统计

  通过内置安全规则，精准识别爆破、SQL 注入、Log4j 等多种类型攻击访问，支持统计最近一小时内的攻击次数和攻击类型。

- 流量分析

公共资源交易平台投标专用
AE2019CE27646E1A62A8BC88EA14DB9

通过拷贝流经核心路由器的全部流量，实时分析并通过图表呈现不同时段流入和流出的流量值及所属 IP 等信息。

- 日志分析

  支持攻击事件日志、阻断日志、流量日志和审计日志，全面记录攻击源和攻击目的的详细信息，帮助运维人员精准定位网络攻击。

- 访问防护

  内置华为云平台多年攻防实战积累的经验规则，覆盖常见网络攻击，并持续运营刷新，有效保护资产，并提供观察和拦截两种防护模式。

- 威胁情报

  通过利用行业威胁情报和华为云自研的大数据量、高准确度的威胁情报库，锁定攻击 IP 的地理位置信息，为精准防护提供进一步的保障。

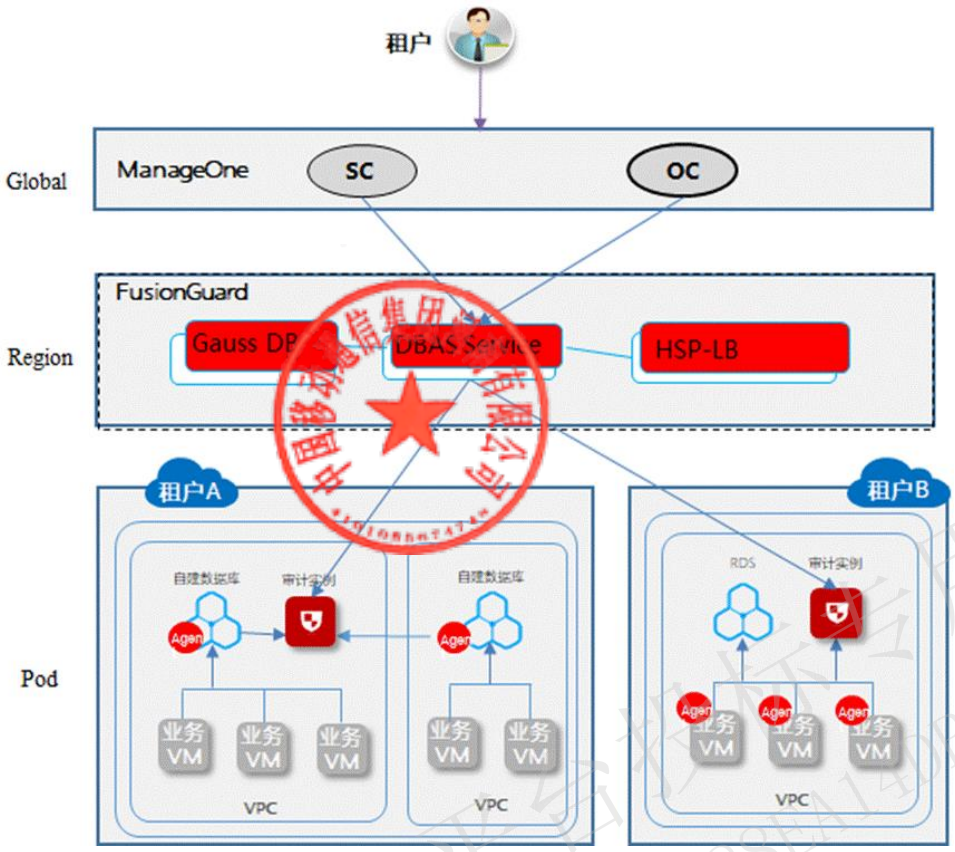
- 告警通知

  当前支持攻击告警通知，当网络攻击达到告警阈值，NDR 将以告警形式上报到 ManageOne 运维面，便于统一运维。

3.8.1.11 虚拟数据库审计

数据库审计服务(Database Audit Service)，为用户的基于 ECS/BMS 自建数据库、RDS 数据库，提供用户行为发现审计、多维度分析、实时告警和报表等功能，保障云上数据库的安全，满足用户合规要求。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9



数据库审计流程

审计信息展示：数据库审计的审计内容包括会话的终端信息、会话的主机信息、会话的其它信息、操作信息等；支持从会话维度、语句类型纬度、风险纬度三个纬度进行导航展示，支持基于时间、客户端 IP、目标数据库 IP、客户端 MAC、目标数据库 MAC，操作类型、客户端端口、操作信息大小、返回状态、结果信息、客户端执行命令等详细信息内容。

审计报表：支持（系统级）多数据库聚合报表展现和单数据库综合性报表展现；支持基于总体概况、性能、会话、语句、风险多层面展现报表；支持报表定时推动功能，自定义推送周期推送报表文档；支持多种关联分析，对异常行为体统精细化报表，如会话（客户端和数据库用户）行为报表、风险操作风险分布情况分析报表、合规报表（满足数据安全标准如 Sarbanes-Oxley）等；

风险操作、攻击检测及告警：风险操作（操作类型、操作对象、风险等级等）告警；能够检测 SQL 注入（命令特征或风险等级）发现并告警；系统资源（CPU、内存和磁盘）阈值告警；支持自定义风险规则。

管理员三权分立：支持系统、安全、审计管理员三员权限分离，并基于云 IAM

进行统一身份认证管理；

隐私数据保护：用户可以通过内置规则或自定义规则对审计平台（审计日志）存储和展示的敏感信息脱敏；严控个人数据收集、存储；

合规及认证：国内：满足网安法、等保三级数据库审计需求，获得公安部《计算机信息系统安全专用产品销售许可证》；国外：满足 SOX、Sarbanes 等国外法案，通过 CSA STAR、ISO 27001、ISO27017、ISO27018 安全认证。

3.8.1.12 **虚拟密码机**

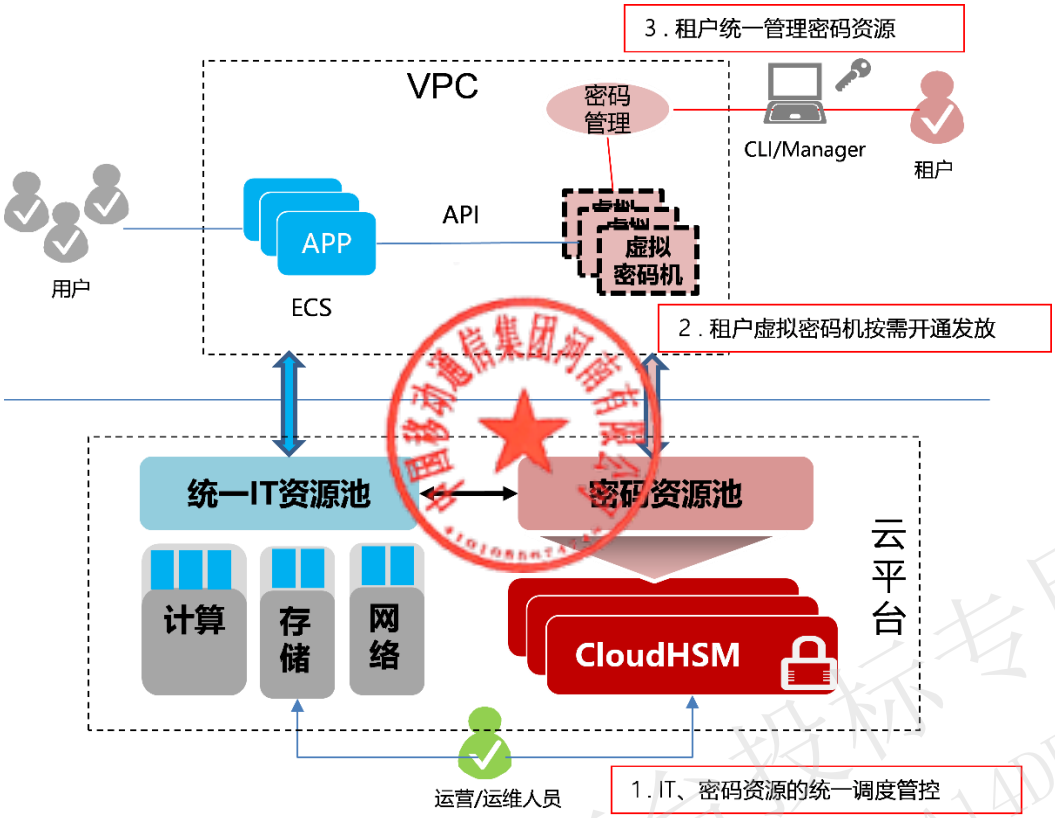
CHSM 云服务器密码机 （cloud-hosted hardware security module，简称 CloudHSM 或 CHSM） ，即在云计算环境下，采用虚拟化技术，以网络形式，为多个租户的应用系统提供密码服务的密码设备。

当前华为云 Stack 数据加密服务支持的云服务器密码机型号为三未信安 SJJ1212、江南天安 SJJ19151，设备均支持国密算法（SM1、SM2、SM3、SM4 等），并获得国家密码局认证。

3.8.1.13 **数据库加密服务**

数据加密服务（Data Encryption Workspace，简称 DEW），基于国家密码局认证的云服务器密码机（CloudHSM），构建虚拟化密码资源池，实现 IT、密码资源统一调度管控，为用户按需提供虚拟密码机（VSM）的服务，支持政务、金融、公安等行业客户的云上密码服务及国密改造需求。解决了加密机入云、密码及 IT 资源统一调度、自动化管维的问题。

公共资源交易平台投标专用
AE2C15CE0276F6E1A6248BC88EA1ADB5



数据加密服务基于云加密机在云平台侧实现了虚拟化密码资源池的构建，并可统一调度管理密码资源，实现 IT、密码资源的统一调度分配，支持对虚拟密码资源的配置、操作、漂移、升级等。租户在数据加密服务界面，可按需申请相应的 VSM 资源，服务自动化将 VSM 设备映射入租户 VPC，同时管理员将所需的管理、备份 Ukey 发放给用户。用户持 Ukey 登录管理配置工具，远程初始化、配置 VSM，并完成应用改造接入，实现应用对加密服务调用。租户可在服务界面进行 VSM 的申请、维护、关闭等，也可登录管理配置工具对名下所有密码设备、密钥进行统一管理和配置。

DEW 服务具有以下功能：

- 密码资源池的统一调度：
  - 实现密码资源池管控系统，基于 CloudHSM 构建密码资源池；
  - 支持对 CloudHSM、VSM 自动化配置、操作、漂移、升级等；
  - 支持对密码资源池统一监管、分配、运维、告警处置等；
  - 支持 VSM 集群集容量：>10240。

公共资源交易平台投标专用

- 租户按需动态开通 VSM：
  - 支持租户自动化开通、配置、关闭 VSM 资源；
  - 支持租户 VSM 资源总览、性能查看、VSM 资源查看等；
  - 单 VSM 加密性能规格：并发连接数 64、256 位 SM2 签名速度 ≥ 3200 次/秒、 SM4 加密/解密速度 ≥ 4000 次/秒、 SM3 杂凑计算性能≥ 4500 次/秒
- 将 VSM 的安全接入租户 VPC：通过网络映射，将 VSM 接入租户 VPC，实现加密机的本地调用，保障 VSM 的使用、管理安全。
- 租户密码资源统一管理：支持租户统一管理名下的所有密码设备、密钥资源。

3.8.2 新增安全服务

3.8.2.1 云资源监控

ManageOne 支持对云平台的各类云资源进行监控，提取各类云资源的监控指标，并支持设定阈值产生相应的阈值告警。

3.8.2.2 数据安全服务DSC

数据安全中心服务（Data Security Center，DSC）是新一代的云化数据安全平台，提供数据分级分类、敏感数据识别、数据水印溯源和数据静态脱敏等基础数据安全能力，通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。

公开资源交易平台投标专用



敏感数据自动识别分类

从海量数据中自动发现并分析敏感数据使用情况，基于数据识别引擎，对其储存结构化数据（RDS）和非结构化数据（OBS）进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。

数据脱敏保护

通过多种预置脱敏算法+用户自定义脱敏算法，搭建数据保护引擎，实现非结构化数据脱敏储存，结构化数据静态脱敏，防止敏感数据泄露。

满足信息合规要求

DSC 拥有数十种合规模板，包含 GDPR，PCI DSS，HIPAA 等，多种合规规则一键匹配识别，生成报表供针对性整改，精准区分和保护个人数据，避免产生合规问题。

功能特性	说明
数据安全总览	展示数据安全全生命周期各个阶段的状态，包括云服务全景图、数据采集安全、数据传输/存储安全、数据使用安全和数据交换/删除安全，实时呈

公共资源交易平台投标专用

功能特性	说明
	现了用户资产的具体情况。
资产列表	DSC 支持管理 OBS、数据库和大数据三类数据资产。
敏感数据识别	• **数据自动分级分类：**在 AI 和专家知识库的双重加权下，精准识别敏感数据和文件，覆盖结构化（RDS）和非结构化（OBS）两种数据类型，实现云上多场景覆盖。 – 文件类型：支持近 200 种非结构化文件。 – 数据类型：支持数十种个人隐私数据类型，包含中英文。 – 合规模板：多种内置合规知识库，如 GDPR，PCI DSS，HIPAA 等。 • **自动识别敏感数据** – 自动识别敏感数据及个人隐私数据。 – 支持自定义规则，场景适配不同行业。 – 血缘图梳理敏感文件框架，清晰定位。
数据脱敏	DSC 的数据脱敏支持静态脱敏和动态脱敏。 DSC 的数据静态脱敏特点： • 不影响用户数据：从原始数据库读取数据，通过精确的脱敏引擎，对用户的敏感数据实施静态脱敏，脱敏结果另行存放，不会影响原始的用户数据。 • 支持云上多种场景：支持 RDS，ECS 自建数据库，大数据。 • 满足多种脱敏需求：用户可以通过 20+种预置脱

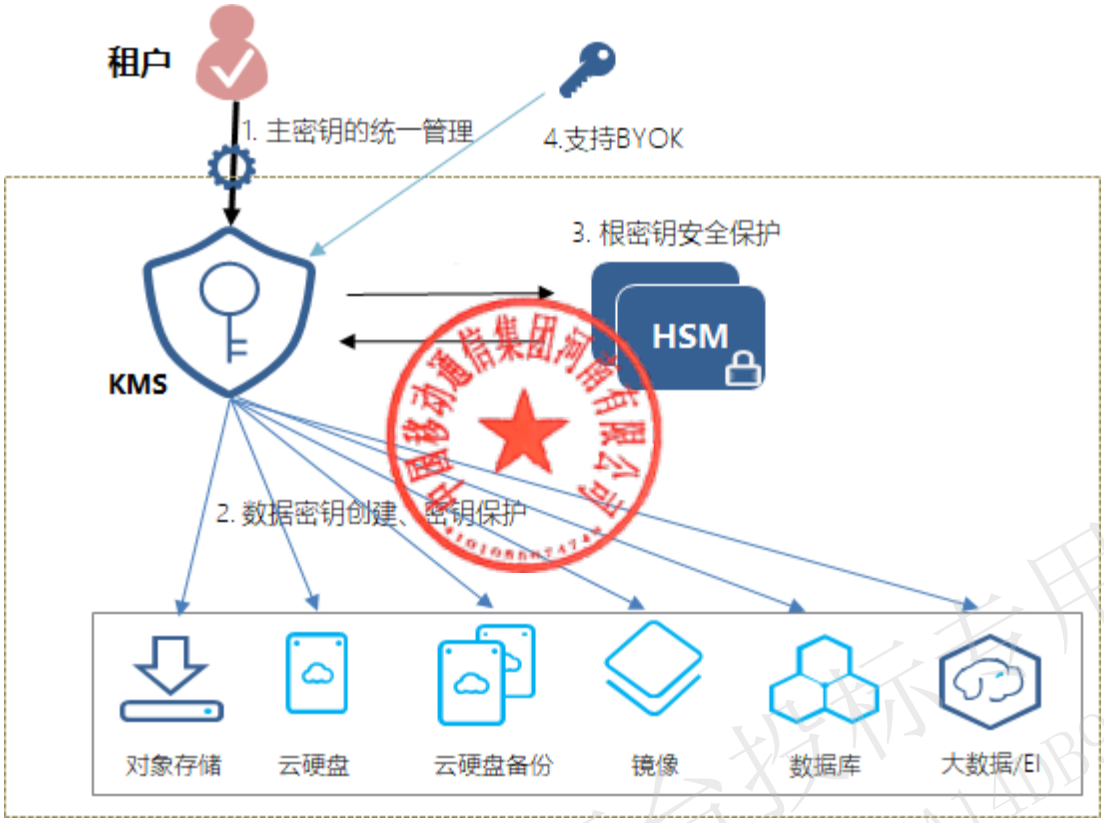
公共资源交易平台投标专用
AE2C19CEC776461462A8BC88EA14DB9

功能特性	说明
	敏规则，或自定义脱敏规则来对指定数据库表进行脱敏实现一键合规。 同时，DSC 提供了数据动态脱敏的 API 接口供您使用。
数据水印	针对 PDF、PPT、Word、Excel 格式的文件提供了添加和提取水印的功能。 • **版权证明：**嵌入数据拥有者的信息，保证资产唯一归属，实现版权保护。 • **追踪溯源：**嵌入数据使用者的信息，在发生数据泄露事件时，追踪其泄露源头。

3.8.2.3 密钥管理服务KMS

密钥管理服务（Key Management Service，简称 KMS）：为平台云服务、租户业务应用提供一种安全可靠、简单易用的密钥托管服务，其密钥安全由硬件安全模块（HSM）保护，帮助用户集中管理密钥生命周期安全。解决了云服务加密密钥安全创建、租户密钥统一管理的问题，当前已支持 OBS、DWS、DAYU 服务集成加密功能。

公共资源交易平台投标专用
AE2C19CEC7764CE1162A8BC88EA14DB9



用户可登录 KMS 系统，对租户住密钥进行全生命周期管理，包含创建、启用、禁用、删除、轮转、别名、修改用户主密钥等。对于集成了 KMS 加密的 OBS 服务，用户登录 OBS 服务时，可以选择“KMS 加密”加密文件，自动对上传文件加密保存在云端存储，下载时自动解密。

KMS 服务具有以下安全功能：

- 密钥生命周期管理：
  - 支持根密钥保护，基于硬件 HSM 根密钥保护。
  - 支持租户创建、启用、禁用、删除、轮转、别名、修改用户主密钥。
  - 支持各服务、应用创建、加密、解密数据密钥。
  - 支持 AES 256、国密 SM4 两类对称密钥的创建和管理。
- 云服务集成加密支持：

- 对象存储服务（OBS）集成：一键开通文件加密功能，对上传/下载 OBS 文件进行服务端加密/解密，1 个文件 1 个密钥。

- 智能数据湖运营平台（DAYU）集成：创建 MRS Hive、MRS Hbase、DWS、DLI、MySQL、SparkSQL、RDS 等数据连接时，自动调用 KMS 创建数据密钥加密数据连接口令等。

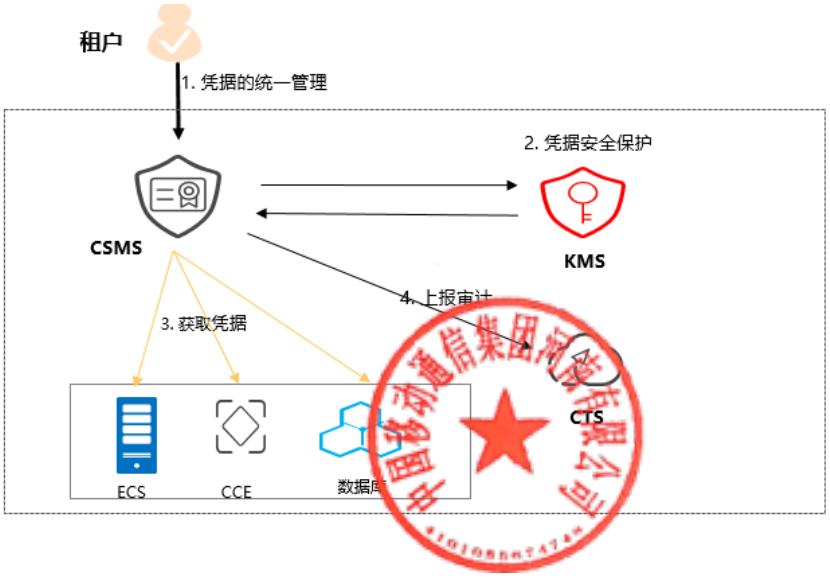
- 数据仓库服务（DWS）集成：服务创建数据表时，自动调用 KMS 创建数据密钥加密数据表。

- 密钥安全管理：
  - 密钥轮转：用户可按需对主密钥进行轮转（支持轮转周期 7 天 ~ 1095 天）；
  - 密钥授权：支持按需密钥授权；
- 自主密钥导入（BYOK）：用户根据 KMS 提供的 API 接口导入用户自己生成或获取到的用户主密钥；
- 小数据加密：少量数据（如口令、证书等）需要加解密时，可利用 KMS 在线工具完成；

当前 KMS 已与国内主流的加密厂商 HSM 设备型号适配：支持江南天安 SJJ1310、三未信安 SJJ1212。

3.8.2.4 凭据管理服务CSMS

公共资源交易平台投标专用



云凭据管理服务（Cloud Secret Management Service，CSMS），是一种安全、可靠、简单易用的凭据托管服务。用户或应用程序通过凭据管理服务，创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期和统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密以及权限失控带来的业务风险。

功能	服务内容
凭据全生命周期管理	• 创建、查看、定时删除、取消删除凭据 • 修改凭据的加密密钥和描述信息
凭据版本管理	• 创建、查看凭据版本 • 查看凭据值
凭据版本状态管理	更新、查询、删除凭据版本状态
凭据标签管理	添加、搜索、编辑、删除标签

以最基础的数据库用户名及密码管理为示例，为您介绍凭据管理服务基本的使用场景。

公共资源交易平台技术专用
AE2619CEC77646E1462A8BC88EA14DB5



流程说明如下：

步骤 1 您首先需要在凭据管理服务中使用控制台或者 API 创建一个凭据，用来存储数据库的相关信息（例如：数据库地址、端口、密码）。

步骤 5 当您使用应用程序访问数据库时，凭据管理服务会去查询步骤 1 所创建的凭据存储的内容。

步骤 6 凭据管理服务检索并解密凭据密文，将凭据中保存的信息通过凭据管理 API 安全地返回到应用程序中。

步骤 7 应用程序获取到解密后的凭据明文信息，使用这些安全的信息访问数据库。

----结束

对其他云服务的依赖：凭据管理的安全能力强依赖于 KMS 服务，当前国内支持 KMS_江南天安、KMS_三未信安，国外 KMS_Utimaco。

3.8.2.5 安全指数服务SIS

安全指数（Security Index Service，SIS）是关于云环境的一个安全评估服务，为用户提供统一、直观、多维度的安全视图。用户可以通过安全指数服务了解所使用云环境是否已合理配置，所采取的安全措施是否已经足够，以及主动安全、被动安全的概况。

- 安全体检：从身份鉴别、访问控制、入侵防范、资源控制、备份恢复、数据安全几个维度对用户的云环境进行评估，根据最佳实践对不安全的配置提出修改建议，并提供快速修复的链接。

公共资源交易平台投标专用

- 合规报告：根据等级保护规范的技术要求，从安全计算环境、安全通信网络维度对用户的云环境进行检测，提供合规检测报告，辅助用户做等保评估。
- 对云服务配置进行检查，依赖 OBS、VPC、BMS、ELB、HSS、VDC、ECS、CSBS、CSDR、KMS、DEW、EdgeFW、CFW 等服务。



3.8.2.6 安全云脑SecMaster

安全云脑（态势感知）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。



安全云脑功能介绍：

总览

总览呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。

功能模块	功能详情
安全评分	根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
安全趋势	呈现最近 7 天整体资产安全健康得分的趋势图。

工作空间管理

工作空间属于云脑顶层工作台，单个工作空间可绑定普通项目、企业项目和 Region，可支撑不同场景下的工作空间运营模式。

功能模块	功能详情
工作空间	单个工作空间可绑定普通项目、企业项目和 Region，可支撑不同场景下的工作空间运营模式。

安全态势

支持通过安全态势即时查看大屏、定期订阅安全运营报告，了解安全运营核心关注指标。

公共资源交易平台投标专用

功能模块		功能详情
态势总览	安全评分	根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况。 评估得分越低，即风险值越大，则整体资产安全隐患越大。
	安全监控	集中呈现未处理的威胁告警、漏洞和合规检查的风险数目，支持快速查看威胁告警、漏洞和合规风险详情。
	安全趋势	呈现最近 7 天整体资产安全健康得分的趋势图。
安全大屏		利用 AI 技术将海量云安全数据的分析并分类，通过安全大屏将数据可视化展示，集中呈现云上实时动态，云上关键风险一目了然，掌握云上安全态势更简单，更直观，更高效。
安全报告		通过创建分析报告，及时掌握资产的安全状况数据。
任务中心		集中呈现当前需要进行处理的任务。

资产管理

安全云脑支持对云上资产全面自动盘点，并呈现云上资产实时安全状态。

功能模块	功能详情
资产管理	同步所有资源的安全状态统计信息，支持查看资源的名称、所属服务、安全状况等，帮助您快速定位安全风险

公共资源交易平台投标专用

功能模块	功能详情
	问题。

风险预防

风险预防提供基线检查和漏洞管理功能，帮助您的云安全配置达到等保等各类权威安全标准和华为云安全最佳实践标准；知晓全局的漏洞分布，并一键修复漏洞。

功能模块	功能详情
基线检查	1、通过执行云服务基线扫描，检查基线配置风险状态，告警提示存在安全隐患的配置，并提供基线加固建议。 2、当前仅支持云服务基线检查，比如 IAM、ECS、OBS、HSS、VPC、WAF、ELB、RDS、DCS、DDOS、VSS 和 CSS
漏洞管理	通过自动同步华为云主机安全服务（Host Security Service，HSS）漏洞扫描数据，分类呈现漏洞扫描详情，支持查看漏洞详情，并提供相应漏洞修复建议。

威胁运营

威胁运营提供丰富的威胁检测模型，帮助您从海量的安全日志中，发现威胁、生成告警；同时，提供丰富的安全响应剧本，帮助您对告警进行自动研判、处置，并对安全防线和安全配置自动加固。

功能模块		功能详情
安全	查询与	• 检索分析：支持数据的快捷检索分析，支持安全调查

公共资源交易平台投标专用

功能模块		功能详情
分析	分析	场景安全数据的快速筛留、筛除等操作，快速定位关键数据。 • 筛选统计：支持数据字段快速分析统计，并基于分析结果进行数据的快速筛选；时序数据支持默认时间分区统计，快速识别数据量的变化趋势，支持基于时间分区的快速筛选；支持分析、统计、排序等丰富统计分析函数，支撑快速构建安全分析模型。 • 可视化：支持数据可视化分析，直观反映业务结构性和趋势性特征，并基于此构建自定义分析报告和分析指标。
	数据监控	支持数据流量端到端的监控管理。
数据监控		支持构建告警模型。
事件管理		集中呈现事件详情，支持人工转事件、自动化转事件。
告警管理		提供统一的数据类管理（安全运营对象），内置华为云告警标准。通过集成各云服务告警，包含 HSS、WAF、DDoS 等，集中呈现告警信息。
情报管理		提供统一的数据类管理（安全运营对象），内置华为云威胁情报指标库标准。支持接入各云服务情报，同时也

公共资源交易平台投标专用
4E2C19CEC7764FE1A62A8BC88EA14DB9

功能模块		功能详情
		可以基于告警和事件自定义规则提取指标。

安全编排

安全编排支持剧本管理、流程管理、数据类管理（安全实体对象）和资产连接管理等。通过安全编排可以对安全、应剧本进行拖拽式的灵活编排，动态适配您的业务需求。也可以对安全运营的对象、交互的页面进行灵活扩展和定义。

功能模块	功能详情
运营对象	集中对数据类、数据类类型、分类映射等运营对象进行管理。
剧本编排	支持对剧本、流程、资产连接、实例的全生命周期管理。
页面布局	提供安全可视化低代码开发平台，基于此平台可自定义安全分析报告、告警管理、事件管理、漏洞管理、基线管理、威胁情报指标库管理等页面布局。

数据集成

通过集成云原生安全产品，进行数据对接。集成后可以检索并分析所有收集到的日志。

功能模块	功能详情
数据集成	云内置采集系统，支持一键集成存储、管理与监管、安全等多种华为云云产品的日志数据。集成后，可以检索

公共资源交易平台投标专用

功能模块	功能详情
	并分析所有收集到的日志。

3.8.2.7 安全组

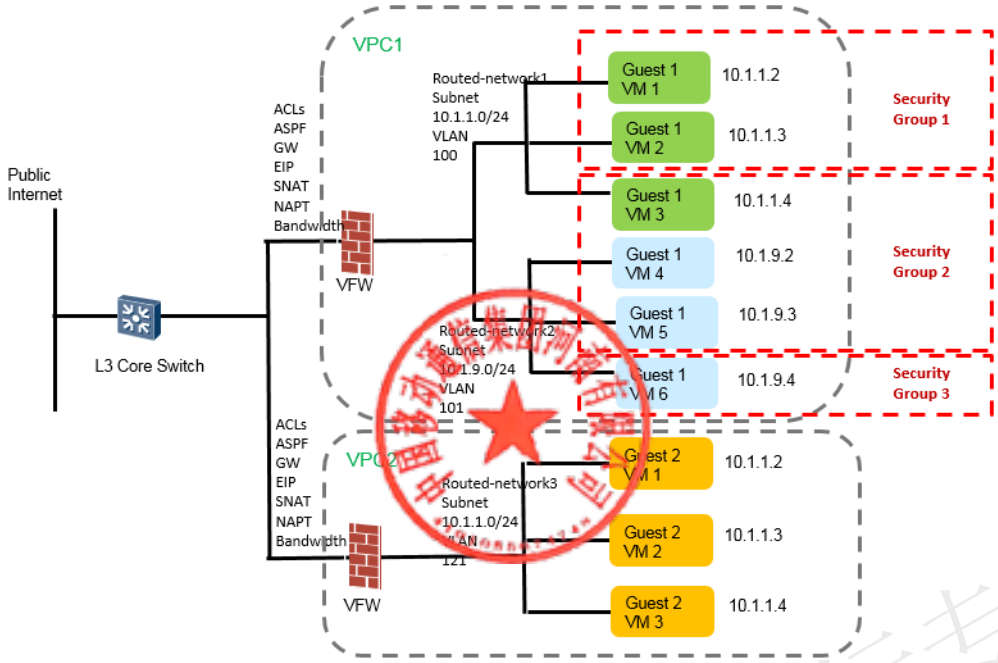
虚拟机可以加入安全组，安全组来实现组内和组间的访问控制，加强虚拟机的安全保护，实现 VPC 内部的网络隔离。安全组通过配置安全规则来控制云主机网络消息的流入流出，只允许授权的消息通过。

系统存在一个默认安全组(default)，当项目管理员创建虚机不指定安全组的时候，系统会自动分配默认的安全组。管理员可以创建自定义的安全组，可以在安全组中定义各种访问规则，当创建一个新的安全组时默认有以下几条规则：

- 允许 IPv4 出方向访问；
- 不允许 IPv4 入方向访问；
- 同一个安全组成员可以互相访问；
- 不同安全组成员不可以互相访问；

安全组默认的一个规则是 Drop，当报文在一个安全组内不能匹配任何规则时，此报文会被丢弃。

公共资源交易平台投标专用
AE2C19CEC7646D1A62A8BC88EA14B29



3.8.2.8 网络ACL

网络 ACL（NetACL）是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。网络 ACL 与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络 ACL。安全组对弹性云服务器进行防护，网络 ACL 对子网进行防护，两者结合起来，可以实现更精细、更复杂的安全访问控制。

NetACL 支持与子网绑定，一个 NetACL 支持和多个子网绑定，一个子网不能同时加入两个 NetACL。

- 支持配置五元组。
- 支持一个防火墙实例关联多个 VPC。
- 防火墙与安全组差异对比

对比项	安全组	网络 ACL
防护对象	弹性云服务器级别操作	子网级别操作

公共资源交易平台投标专用

对比项	安全组	网络 ACL
配置策略	仅支持允许策略	支持允许、拒绝策略
优先级	多个规则冲突，取其并集生效。	多个规则冲突，优先级高的规则优先生效。
应用操作	创建弹性云服务器默认必须选择安全组，默认安全组自动应用到弹性云服务器	创建子网没有网络 ACL 选项，必须创建网络 ACL、添加关联子网、添加出入规则，并启用网络 ACL，才可应用到关联子网及子网下的弹性云服务器
报文组	仅支持报文三元组（即协议、端口和对端地址）过滤	支持报文五元组（即协议、源端口、目的端口、源地址和目的地址）过滤

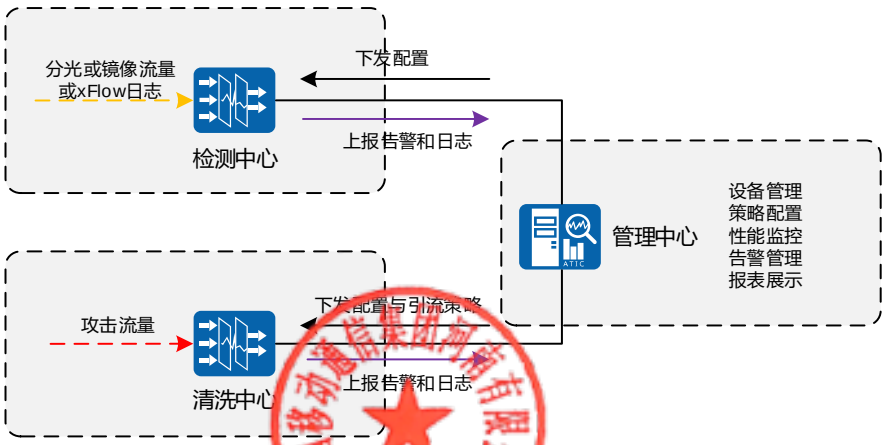
公共资源交易平台投标专用

3.8.2.9 AntiDDos

Anti-DDoS流量清洗（以下简称Anti-DDoS）为公网IP提供四到七层的DDoS攻击防护和攻击实时告警通知。同时，Anti-DDoS可以提升用户带宽利用率，确保用户业务稳定运行。

AntiDDoS 通过对互联网访问公网 IP 的业务流量进行实时监测，及时发现异常 DDoS 攻击流量。在不影响正常业务的前提下，根据用户配置的防护策略，清洗掉攻击流量。同时，Anti-DDoS 为用户生成监控报表，清晰展示网络流量的安全状况。

Anti-DDoS解决方案由华为自主研发的AntiDDoS和管理中心组成。其中AntiDDoS包含检测中心和清洗中心两部分，所以整个方案包括检测中心、清洗中心和管理中心三大部分。



- **检测中心**

检测中心负责对流量进行检测，发现异常后上报管理中心，由管理中心下发引流策略至清洗中心进行引流清洗。检测中心的检测技术主要分为两种，一是基于Netflow的流量检测技术，二是基于应用的逐包检测技术，前者仅能检测大流量攻击，后者不仅能检测出大流量攻击还能够检测出小流量攻击和应用层攻击。

- **清洗中心**

清洗中心主要根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。清洗中心提供多种DDoS流量清洗手段，可以准确识别正常流量，清洗各类异常流量，包括流量型攻击、应用层攻击、扫描窥探型攻击及畸形包攻击。清洗中心同时具备检测中心的功能，当业务对检测清洗性能要求较低时可只部署清洗中心。

- **管理中心**

管理中心，负责检测中心和清洗中心的统一管理，是Anti-DDoS解决方案的管理中枢。提供设备管理、策略管理、性能管理、告警管理、报表管理等功能。

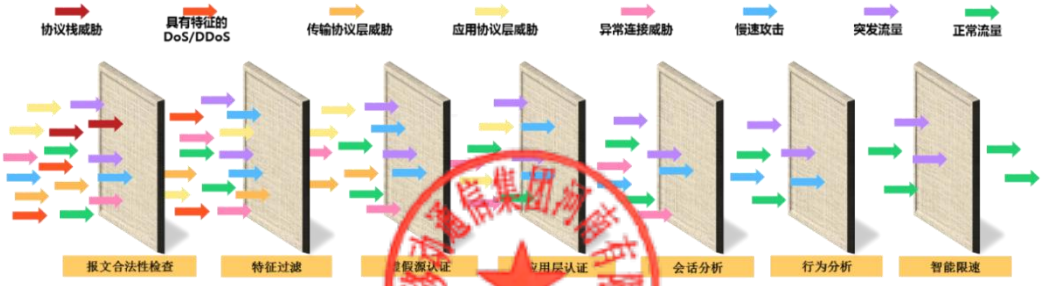
- **功能介绍**

手术刀式多层防范机制

移动清洗系统提供了逐层防范机制，使用报文合法性检查，特征过滤，虚假源认证，应用层认证，会话分析，行为分析，智能限速多种防范技术对流量

公共资源交易平台投标专用

进行层层筛选，保证攻击流量能够被相应算法识别并丢弃。其强大的防范机制可以灵活应对当前多变的DDoS攻击现状，为服务器提供100%的安全保证。



报文合法性检查

Anti-DDoS系统能够针对网络中的报文合法性做检查，针对违反RFC等协议标准的报文将直接丢弃，避免其可能对服务器造成的性能损耗。同时设备配备的强大DoS防范功能可以轻松应对LAND，Fraggle等常见传输层畸形包攻击，为服务器提供第一层安全保障。用于防范：Smurf攻击，Land攻击，Fraggle攻击，IP分片报文攻击，IP欺骗攻击，Ping of Death攻击， TCP报文标志位攻击，Teardrop攻击，WinNuke攻击。

特征过滤

基于大部分DDoS攻击均具有固定特征这个特点，移动开发了强大的特征过滤功能，能够针对源IP，协议，端口，负载，应用协议特定字段等信息进行匹配和过滤，实现对网络流量的灵活控制。同时搭配移动自研的动态指纹发现技术和抓包文件指纹自提取技术，减少了管理员手工介入防范的工作量，提高了应急响应效率。

利用特征过滤功能，移动Anti-DDoS系统集成了部分僵木蠕防范功能，用以防范经常伴随DDoS攻击出现的各种入侵，后门，远程控制行为。使用移动安全能力中心发布的特征库可以针对100+种流行的网络攻击进行防护。如UDP Flood、UDP类反射放大攻击（包括DNS反射放大，NTP反射放大等）。

虚假源认证

Anti-DDoS系统支持众多源认证算法，既包括syn cookie等业界通用防范算法，也包含了源IP信誉算法等一批具有移动自主知识产权的验证算法。清洗设备可以应用这些算法轻易的将虚假主机和正常访问客户区分开，有效避免屏蔽

公共资源交易平台技术专用

大量的虚假源IP攻击，形成源认证防范的第一道屏障。用于防范虚假源发起的SYN Flood。

应用层认证

对于使用僵尸主机自身IP发起的攻击行为，移动提供大量的独特算法通过对应用层交互行为的检查来有效区分僵尸主机和正常访问客户，完成对正常用户的认证工作。同时搭配终端识别技术，可以获取客户端的详细信息，并根据不同客户端对应用协议的支持情况分别使用独立算法，有效降低了流量清洗出现误判的几率。用于防范虚假源或僵尸工具发起的DNS Query Flood、DNS Reply Flood、HTTP get/post Flood、HTTPS Flood、SIP Flood。

会话分析

移动清洗中心能够通过监控网络流量的实时信息，并记录于清洗系统专有的会话中。通过会话检测可有效防范TCP类异常会话攻击如慢速攻击、重传攻击、慢启动攻击，亦可有效防范DNS缓存投毒攻击、DNS反射攻击。在应用层DDoS攻击发展迅速的今天，会话分析将是一种重要的防范技术。用于防范如ACK Flood、FIN/RST Flood、TCP连接耗尽攻击、socktress、重传攻击、DNS Cache Poisoning、SSL-DoS/SSL-DDoS、 HTTP slow headers/post attack。

行为分析

僵尸网络的攻击行为和正常用户的访问行为存在很大差别，主要表现在正常用户的访问具有突发性及无序性，而僵尸网络的攻击属于机器人攻击，频率恒定，或者访问的资源基本保持不变，或者TCP流量比率异常，或者攻击报文负载不变，移动清洗设备能够采用指纹学习或访问频率行为学习来防范该类攻击。用于防范CC攻击、慢速SYN Flood。

智能限速

Anti-DDoS系统能够智能的对网络中的IP流量和应用层流量进行分析，对于流量大于特定值的流量能够实施基于源IP，目的IP，报文类型，特定字段的限速。以实现对整网流量的可控，可限，保证后端服务器在大量正常流量冲击下任能提供服务。

公共资源交易平台投标专用

灵活的部署

移动Anti-DDoS产品提供强大的路由和转发功能，保证了在复杂的客户网络中总是能够合理的部署DDoS防护系统。

引流技术

移动提供业界最强大的BGP路由功能，在Anti-DDoS方案中可以灵活的针对流量进行牵引，并通过路由策略准确的控制路由发布。而BGP邻居安全认证技术则保证了BGP连接的安全。同时移动也提供了策略路由，IGP等其它的引流技术以供特定场景使用。另外，移动引入了动态引流，静态引流，手工引流等多种引流方式，提供流量牵引的灵活性。

回注技术

在做旁路部署时，流量如何回注一直是Anti-DDoS系统部署的难题。为了应对此问题，移动Anti-DDoS清洗设备支持丰富的回注技术，包括MPLS，MPLS L3 VPN，GRE，802.1q，PBR。其中MPLS和MPLS L3 VPN能够应对复杂组网要求，其余技术针对网络边界防护能够提供有效支持。

高可靠

为了应对网络设备可能突发的故障问题，移动Anti-DDoS解决方案提供了一整套高可靠性技术。

- **方案级可靠性：**

逐包检测+动态引流清洗：

通过分光/镜像复制一份流量到Anti-DDoS设备进行检测，发现异常后发送主机路由动态引流受攻击地址的流量到Anti-DDoS进行清洗。无论是检测中心、清洗中心、管理中心或者DDoS系统网元间的连接故障，都只会导致Anti-DDoS系统暂时无法提供DDoS防护能力，管理员可以根据Anti-DDoS相关的故障信息快速修复故障，期间不会对现网业务造成任何影响。

Netflow检测+动态引流清洗：

路由器/交换机发送流量汇总信息（Netflow）给Netflow分析器（GenieATM），Netflow分析器汇总各个路由器/交换机的Netflow信息，发现攻

公共资源交易平台投标专用

击后发送syslog日志给ATIC，ATIC启动引流清洗。无论是检测中心、清洗中心、管理中心或者DDoS系统网元间的连接故障，都只会导致Anti-DDoS系统暂时无法提供DDoS防护能力，管理员可以根据Anti-DDoS相关的故障信息快速修复故障，期间不会对现网业务造成任何影响。

低误判

移动清洗系统为降低清洗对网络影响，提出了基于业务的精细化清洗思路。所有清洗活动以目的 IP，端口和协议为最小粒度，保证其它未受攻击业务直接转发。针对 Anti-DDoS 产品可能出现的误判和错判情况进行了算法改进，提出了包括 DNS 被动源认证等多种改进算法，保证正常业务不会因为清洗而出现中断。针对目前终端设备对应用协议栈支持程度不一这种情况，移动公司提出了终端识别技术等一批终端鉴别技术，针对不同终端和应用将分别使用独立的防范算法，进一步降低了 Anti-DDoS 误判的可能性。

3.8.2.10 **网闸**

网闸，又称为物理隔离网闸，网闸主要是通过在网络模型的各层的断开，例如物理层断开、链路层断开、TCP/IP 协议隔离和应用协议隔离，因此，网闸从逻辑上隔离、阻断了对内网具有潜在攻击可能的一切网络连接，使外部攻击者无法直接入侵、攻击或破坏内网，保障了内部主机的安全。

网闸就是要解决目前网络安全存在的下述问题。

（1）对操作系统的依赖，而操作系统可能有漏洞，存在被攻击的风险；

（2）对 TCP/IP 协议的依赖，而 TCP/IP 协议有漏洞；

（3）解决通信连接的问题，内网和外网直接连接，存在基于通信的攻击；

（4）应用协议的漏洞，如非法的命令和指令等。

3.9 培训方案

3.9.1 培训目标

人员培训作为政务云实施、使用的一个重要环节，因此，我投标方对培训工作极为重视。为了确保系统在使用中稳定、高效率的工作，我投标方在对项目中的各系统技术特点、客户人员状况以及项目实施计划进行具体分析的基础上，针

对各系统的管理、维护、应用以及日常故障的处理，为不同人员提供了一系列行之有效的培训实施方案,安排具有丰富教学经验的教员进行培训。

通过培训要达到以下预期效果：

使各上云单位的业务操作用户，即业务操作人员掌握云资源使用方法和操作技巧，使用户提升云资源操作熟练度。

使各上云单位的技术人员，即系统管理员、运行维护专业技术人员了解和掌握政务云相关操作技术，具备云安全防护基础能力。

增加各上云单位业务管理人员、运行维护人员的知识储备与安全能力。

3.9.2 培训制度

3.9.2.1 培训报名/受理制度

南阳市政务云主管部门根据乙方上报的培训计划，在培训前三天向各用云单位下发培训通知（培训地点及具体时间由甲乙双方协商确定），并要求各单位上报参训人员信息，原则上要求参训人员为部门上云业务管理或维护人员。甲方根据各单位上报人员信息，通知乙方提前准备培训相关资料。

3.9.2.2 培训取消/推迟制度

如甲方不能按照乙方培训计划进行培训通知或临时决定取消、推迟培训，需甲方在培训开始前 3 天（日历日）以书面形式通知乙方，乙方根据培训计划顺延。

3.9.2.3 培训纪律

1）参训人员在培训开始前 15 分钟到场，相关人员负责监督参训人签到，培训讲师应提前 5 分钟到场。

2）参训人员要遵守培训时间的规定，不迟到、不早退，到达培训场所后要自觉签到。

3）因故无法按规定参加培训时，提前向政务云主管部门报备，并要有相关人员签字。

4）培训开始后，培训现场要有培训负责人员或受训部门培训管理员在场负责，以维持纪律，协助讲师顺利完成培训任务。

5）参训时准备好学习工具，一般要带笔、笔记本等。

6）参训时将手机关闭，或将铃声关闭，参训人员不能因为自身原因干扰培训课的正常进行。

公共资源交易平台技术专用

3.9.3 培训计划

服务期内我方每年提供不低于 1 次，不高于 3 次的集中技术培训。培训开始前乙方向甲方提供详细的培训计划安排，甲方对培训计划审核同意后，乙方进行培训计划实施。

3.9.3.1 培训对象

通过对各上云单位的业务管理人员的培训，使其清晰地了解云服务的申请使用流程、使用方法、云网安全等相关知识。

3.9.3.2 培训形式

本项目将采用南阳本地现场集中培训的方式，理论与实践相结合，对客户的技术人员和管理人员进行流程、安全和操作培训。

现场培训旨在针对不同的用户、用户工作、用户环境提供大量小规模、有针对性甚至点对点的系统用户培训。这种培训的特点是针对性强、直观、方式灵活，而且与实际结合紧密，用户在培训中的问题可以及时得到解答。

3.9.3.3 培训内容

南阳市政务云申请流程；

南阳市政务云操作使用指南；

南阳市政务云网络安全责任划分；

南阳市政务云网络安全及防护；

南阳市政务云密码服务使用指南；

弹性云服务器的功能特性及应用场景；

弹性云服务器的基本操作及特性应用；

南阳市政务云镜像管理服务；

镜像管理服务的功能特性及应用场景；

镜像管理服务的基本操作等政务云服务内容使用培训。

3.9.4 培训师资

我方培训讲师均拥有华为认证培训资格，讲师分为专职教师和兼职教师。

专职教师：华为培训中心有 300 余名专职培训教师，80%以上具有硕士以上学位，具有丰富的研发和运维实践经验，具有最前沿的专业知识和出色的教学技

公共资源交易平台 投标专用

能。所有在岗教师均经过严格的资格认证与考核。

兼职教师：培训中心长期聘请一些经过资格认证、富有经验的研发专家和工程维护专家担任兼职教师，在教学中带给用户更新更深层的产品知识和实用的维护经验。

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

3.10 **对技术要求的承诺书**

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

（1）我公司承诺配合采购人做好政务云监管平台接入及政务云安全工作，确保本项目达到国家监管部门要求。

（2）我公司承诺在签订合同后按工期完成云服务平台安装部署，并具备服务能力。

（3）我公司承诺无条件配合做好各单位业务应用迁移上云工作。

（4）我公司承诺未经允许不得对云平台上的任何数据进行截取、加工、分析和处理，或提供给第三方。

（5）我公司承诺在服务期结束后，无条件配合各使用单位迁移应用系统，提供服务退出承诺书。

（6）机房要求：我公司提供云平台需要的机房环境，包含安全可控的独立机房区域、电力、机柜、制冷、门禁及视频监控等，标准为国标 A 级。

（7）云管理平台要求：通过云管理平台软件对资源进行管理，提供弹性计算、自动化部署、资源区域划分等功能，通过统一的接口为云运营平台和云监管平台提供相关功能要求。

（9）基础安全要求：符合《信息安全技术云计算服务安全指南》

公共资源交易平台投标专用

(GB/T31167-2014)、《信息安全技术 网络安全等级保护实施指南》(GB/T25058-2019)、《信息系统密码应用基本要求》(GM/T0054-2018)等规范要求，政务云平台应通过信息安全等级保护三级认证、商用密码应用安全性评估、云计算服务安全评估。政务云平台应在不同层面保障政务云安全，包括基础设施安全、云平台安全、云租户安全、平台运维安全、平台合规审计等，并提供网络隔离、租户隔离、漏洞扫描、主机安全、日志审计、通用密码、数据库加密等安全及密码能力。采购的云计算服务，相关网络安全部分，如果未有明确要求，按上级政策规定执行。

（10）网络要求：我公司提供 SDN、VxLAN 相关网络服务，支持与互联网、电子政务外网及行业部门专网的连接。提供与电子政务外网核心交换节点连接的专线。

（11）我公司已按照采购人要求，提供详细的技术实施方案。

（12）我公司承诺配合各政务部门使用政务云或者迁移应用系统至政务云平台等相关工作，主要负责但不限于如下工作：

1）配合各单位应用系统迁移前的环境需求分析工作。

2）负责各单位应用系统迁移前的测试环境搭建工作。

3）配置物理服务器、配置虚拟机、配置网络、安装操作系统、配置相应的安全策略等。

4）配合或提供各单位应用系统迁移需要使用的迁移工具。

5）配合各单位应用系统迁移过程中遇到问题故障分析以及提出解决方案，并配合解决问题故障。

公共资源交易平台投标专用

6）负责各单位应用系统迁移过程中对硬件、网络、软件、安全等运行环境的变更工作。

7）我公司承诺配合各单位应用系统迁移后进行测试工作，如压力测试、故障测试等。

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

四、拟投入本项目的运维人员名单及基本情况

4.1 运维团队专业技术人员信息表

序号	姓名	在本项目担任职务	相关证书	所属公司
1	谌伟超	运维人员	高级工程师	中国移动通信集团河南有限公司
2	高阳	运维人员	高级工程师	中国移动通信集团河南有限公司
3	郭晓玲	运维人员	高级工程师	中国移动通信集团河南有限公司
4	黄伟	运维人员	高级工程师	中国移动通信集团河南有限公司
5	李军	运维人员	高级工程师	中国移动通信集团河南有限公司
6	郝文胜	运维人员	高级工程师	中国移动通信集团河南有限公司
7	蒋纬昌	运维人员	网络工程师、网络安全	中国移动通信集团河南有限公司南阳分公司
8	高锋杰	运维人员	云应用集成交付工程师	中国移动通信集团河南有限公司南阳分公司
9	姚鹏	运维人员	云服务解决方案架构师	华为云计算技术有限公司南京分公司
10	王春光	运维人员	云服务解决方案架构师	北京华为云计算技术有限公司
11	胡辉	运维人员	云服务解决方案架构师	华为技术有限公司北京研究所
12	冯纯硕	运维人员	云服务解决方案架构师	华为安驰智行技术有限公司
13	李东伟	运维人员	云服务解决方案架构师	西安华为技术有限公司
14	张哲千	运维人员	云服务解决方案架构师	华为技术有限公司

4.2 原厂服务承诺函

制造厂商售后服务承诺函

致： 南阳市政务服务和大数据管理局

华为技术有限公司郑重承诺： 作为制造商，对于由我公司制造，并由 中国移动通信集团河南有限公司 为贵方 南阳市政务服务和大数据管理局政务云政府购买服务项目 项目供应的 华为云Stack 产品/设备，在中国大陆区域（不包含香港、台湾及澳门），我公司将提供 叁 年 标准 原厂售后维护服务。在上述售后维护服务期内，我公司承诺对我公司制造的上述产品/设备的主要部件或模块提供以下维护服务：

1. 远程支持服务
   1）Help Desk：华为为客户提供24 小时问题统一受理平台，电话号码为400-822-9999。
   2）远程问题处理：华为为客户提供7*24 远程问题处理服务，就有关设备或网络的技术咨询及问题，进行远程技术支持和处理，并提供问题解决方案。
   3）在线技术支持服务：华为为客户提供网站自助平台，客户以授权用户的身份访问华为公司技术网站（http://enterprise.huawei.com）可访问技术论坛、下载相关软件补丁、还可获取产品技术手册、技术案例、维护经验等。
2. 软件更新服务：为解决软件版本的BUG、功能改进或增强提供软件补丁（外购件除外）。
3. 硬件支持服务：华为确定为硬件故障后，可为客户提供7*10*ND（15:30 前受理的申请将下一日送达）硬件预更换服务（外购件除外）。
4. 提供5-6名原厂运维人员（详细信息另行提供）提供本地支持服务。

上述产品/设备具体实际享有的售后维护服务期限、起始日期及内容以我公司出售该产品/设备时与授权经销商或贵方的正式协议（或订单）约定为准。在售后服务期满后，该服务期内享有的服务自行终止；如用户需要我公司继续提供售后服务，可向我公司购买相应的服务，详见官网链接：http://support.huawei.com/enterprise/servesolution。

华为技术有限公司
2023年12月21日

公共资源交易中心 仅供招标文件专用
AE2C19CEC77646E1B2C88A14DB9

4.3 移动—谌伟超—高级工程师证书及社保证明



从事专业
Speciality 交换技术

专业技术职务任职资格
Professional & Technical Qualifications 高级工程师

评审组织
Organization Of Evaluation 河南省通信工程专业技术职务任职资格评审委员会

评审通过时间
Time Of Adoption 2014.12

发证单位
Issuing Authority 河南省人民政府

文件号 豫职改[2015]17号

姓名 Full Name 谌伟超

性别 Sex 男

出生年月 Birthdate 1975.01

籍贯 Native Place

工作单位 Work Unit 中国移动通信集团河南有限公司

证书编号 Credentials No. B19140900503

年 月 日
2015 4 1

公共资源交易
AE2C19CEC77646E1A62

表单验证号码0cdc5ef15f5b408d869ba2cf22eb4198

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	310107197501075436		
社会保障号码	310107197501075436	姓　名	谌伟超	性别	男

单位名称	险种类型	起始年月	截止年月
中国移动通信集团河南有限公司	失业保险	200305	-
中国移动通信集团河南有限公司	工伤保险	200401	-
中国移动通信集团河南有限公司	工伤保险	200307	200611
中国移动通信集团河南有限公司	企业职工基本养老保险	200612	-
中国移动通信集团河南有限公司	企业职工基本养老保险	200307	200611

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	2003-07-01	参保缴费	2003-05-01	参保缴费	2004-01-01	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	17043	●	17043	●	17043	-
02	17043	●	17043	●	17043	-
03	17043	●	17043	●	17043	-
04	17043	●	17043	●	17043	-
05	17043	●	17043	●	17043	-
06	17043	●	17043	●	17043	-
07	17895	●	17895	●	17895	-
08	17895	●	17895	●	17895	-
09	17895	●	17895	●	17895	-
10	17895	●	17895	●	17895	-
11	17895	●	17895	●	17895	-
12	17895	△	17895	△	17895	-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，○表示外地转入，-表示未制定计划。

4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

打印时间：2023-12-11

公共资源交易平台投标专用

4.4 移动—高阳—高级工程师证书及社保证明



公共资源交易平台 专用
AE2C19CEC77646E1A62A8BC88EA

表单验证号码6e93ae56b8cd4276be362d45f6b45a8b

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	412727198803306533		
社会保障号码	412727198803306533	姓　名	高阳	性别	男

单位名称	险种类型	起始年月	截止年月
中国移动通信集团河南有限公司	企业职工基本养老保险	201308	-
中国移动通信集团河南有限公司	失业保险	201601	-
中国移动通信集团河南有限公司	工伤保险	201308	-

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	2013-08-01	参保缴费	2013-01-01	参保缴费	2013-08-23	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	17043	●	17043	●	17043	-
02	17043	●	17043	●	17043	-
03	17043	●	17043	●	17043	-
04	17043	●	17043	●	17043	-
05	17043	●	17043	●	17043	-
06	17043	●	17043	●	17043	-
07	17895	●	17895	●	17895	-
08	17895	●	17895	●	17895	-
09	17895	●	17895	●	17895	-
10	17895	●	17895	●	17895	-
11	17895	●	17895	●	17895	-
12	17895	△	17895	△	17895	-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，○表示外地转入，-表示未制定计划。

4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

河南省社会保险中心 业务查询专用章

打印时间：2023-12-11

公共资源交易平台技术专用
AE2C15...C776462...1621...8DC9E14DB9

4.5 移动—郭晓玲—高级工程师证书及社保证明



公共资源交易平台 AE2C19CEC77646E1A62A8BC

表单验证号码56162b61589d4503b558f8ca25f6086e

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	410321197710193043		
社会保障号码	410321197710193043	姓　名	郭晓玲	性别	女

单位名称	险种类型	起始年月	截止年月
中国移动通信集团河南有限公司	工伤保险	200401	-
中国移动通信集团河南有限公司	工伤保险	200204	200611
中国移动通信集团河南有限公司	企业职工基本养老保险	200612	-
中国移动通信集团河南有限公司	企业职工基本养老保险	200204	200611
中国移动通信集团河南有限公司	失业保险	200301	-

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	2002-04-01	参保缴费	2002-07-01	参保缴费	2004-01-01	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	17043	●	17043	●	17043	-
02	17043	●	17043	●	17043	-
03	17043	●	17043	●	17043	-
04	17043	●	17043	●	17043	-
05	17043	●	17043	●	17043	-
06	17043	●	17043	●	17043	-
07	17895	●	17895	●	17895	-
08	17895	●	17895	●	17895	-
09	17895	●	17895	●	17895	-
10	17895	●	17895	●	17895	-
11	17895	●	17895	●	17895	-
12	17895	△	17895	△	17895	-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，〇表示外地转入，-表示未制定计划。

4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

打印时间：2023-12-11

公共资源交易平台 技术专用

4.6 移动—黄伟—高级工程师证书及社保证明



公共资源交易平台 AE2C19CEC77646E1A62

表单验证号码8bd8a28bd74944af8e5fad82e4b4eb55

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	413023197301290052		
社会保障号码	413023197301290052	姓　名	黄伟	性别	男

单位名称	险种类型	起始年月	截止年月
中国移动通信集团河南有限公司	企业职工基本养老保险	200406	-
中国移动通信集团河南有限公司	工伤保险	200503	-
中国移动通信集团河南有限公司	失业保险	200404	-

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	2004-06-01	参保缴费	2004-04-01	参保缴费	2005-03-23	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	17043	●	17043	●	17043	-
02	17043	●	17043	●	17043	-
03	17043	●	17043	●	17043	-
04	17043	●	17043	●	17043	-
05	17043	●	17043	●	17043	-
06	17043	●	17043	●	17043	-
07	17895	●	17895	●	17895	-
08	17895	●	17895	●	17895	-
09	17895	●	17895	●	17895	-
10	17895	●	17895	●	17895	-
11	17895	●	17895	●	17895	-
12	17895	△	17895	△	17895	-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，○表示外地转入，-表示未制定计划。

4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

河南省社会保险中心 业务查询专用章

打印时间：2023-12-11

公共资源交易平台 技术专用

4.7 移动—李军—高级工程师证书及社保证明



公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

表单验证号码2098792bdbba4a37bd494a7670b556ea

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	412901197105164550		
社会保障号码	412901197105164550	姓　名	李军	性别	男

单位名称	险种类型	起始年月	截止年月
中国移动通信集团河南有限公司	工伤保险	200803	-
中国移动通信集团河南有限公司	企业职工基本养老保险	199901	-
中国移动通信集团河南有限公司	失业保险	201107	-

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	1999-01-01	参保缴费	1999-01-01	参保缴费	2008-03-14	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	17043	●	17043	●	17043	-
02	17043	●	17043	●	17043	-
03	17043	●	17043	●	17043	-
04	17043	●	17043	●	17043	-
05	17043	●	17043	●	17043	-
06	17043	●	17043	●	17043	-
07	17895	●	17895	●	17895	-
08	17895	●	17895	●	17895	-
09	17895	●	17895	●	17895	-
10	17895	●	17895	●	17895	-
11	17895	●	17895	●	17895	-
12	17895	●	17895	●	17895	-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，○表示外地转入，-表示未制定计划。

4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

河南省社会保险中心 业务查询专用章

打印时间：2023-12-12

公共资源交易平台 仅供查询专用

4.8 移动—郝文胜—高级工程师证书及社保证明



从事专业 互联网技术

取得职称名称 高级工程师

取得职称级别 副高级

取得方式 评审

评审组织（认定部门） 河南省工程系列通信专业副高级职称评审委员会

评审（认定）通过时间 2020.12

发证单位 河南省人力资源和社会保障厅

姓名 郝文胜 性别 男

出生年月 1984.04

工作单位 中国移动通信集团河南有限公司

证书编号 B202009081900045

2021 年 02 月 20 日

公共资源交易平台 AE2C19CEC77646E1A82A8B

表单验证号码1811f84e8e78410985b11f389ceb0276

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	410211198404065031		
社会保障号码	410211198404065031	姓　名	郝文胜	性别	男

单位名称	险种类型	起始年月	截止年月
河南百硕商务服务有限公司	工伤保险	201204	201509
新乡市众望人才资源有限公司	工伤保险	201412	201412
新乡市众望人才资源有限公司	工伤保险	201501	201412
河南百硕商务服务有限公司	失业保险	201204	201509
河南晨阳科贸实业有限公司	企业职工基本养老保险	200811	201104
中国移动通信集团河南有限公司	工伤保险	201711	-
中国移动通信集团河南有限公司	失业保险	201601	-
河南百硕商务服务有限公司	企业职工基本养老保险	201204	201509
中国移动通信集团河南有限公司	企业职工基本养老保险	200606	-
河南众泰人力资源管理服务有限公司	企业职工基本养老保险	201107	201203
河南百硕商务服务有限公司	工伤保险	201510	201509

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	2006-06-01	参保缴费	2011-06-01	参保缴费	2006-06-21	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	17043	●	17043	●	17043	-
02	17043	●	17043	●	17043	-
03	17043	●	17043	●	17043	-
04	17043	●	17043	●	17043	-
05	17043	●	17043	●	17043	-
06	17043	●	17043	●	17043	-
07	17895	●	17895	●	17895	-
08	17895	●	17895	●	17895	-
09	17895	●	17895	●	17895	-
10	17895	●	17895	●	17895	-
11	17895	△	17895	△	17895	-
12		-		-		-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，○表示外地转入，-表示未制定计划。

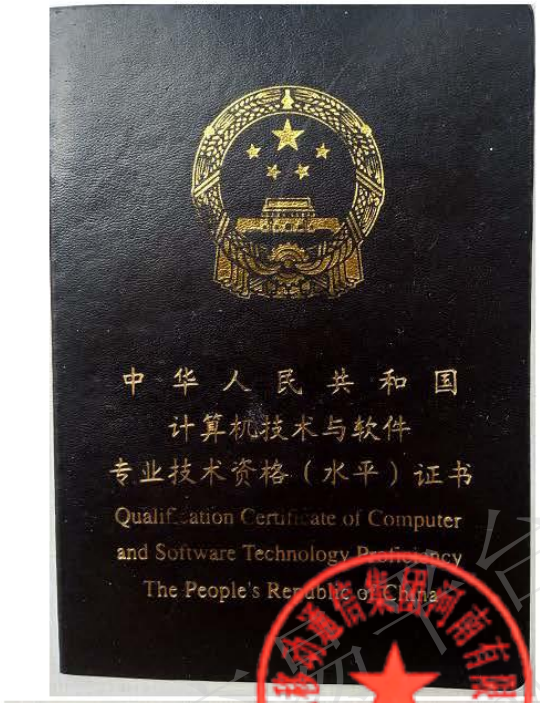
4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

河南省社会保险中心 业务查询专用章

公共资源交易平台 技术专用

4.9 移动—蒋纬昌—网络工程师、网络安全证书及社保证明





公共资源交易平台投标专用
AE2018C8BC88EA14DB9



中国通信企业协会网络安全人员能力认证证书

China Association of Communication Enterprises Cybersecurity Personnel Ability Certificate

本证书由中国通信企业协会批准颁发，表明持证人通过统一的考试和评审，符合《**电信和互联网行业网络安全人员能力认证准则**》的要求，获得相应的网络安全人员能力认证类型和等级的证书。

批准人：

中国通信企业协会

姓　　名：	蒋纬昌
证件号码：	41130219890402341X
工作单位：	中国移动通信集团河南有限公司南阳分公司
类别和级别：	技术类专业级
注册日期：	2022 年 9 月 7 日
有效时间：	2025 年 9 月 6 日
证书编号：	CACE-CPAC-PLT-20220011

公共资源交易平台
AE2C19CEC77646E1A62A8BC88EA

表单验证号码b681da6a9d154152ad99c1d1404d8d67

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	411302198904023 41X		
社会保障号码	411302198904023 41X	姓　名	蒋纬昌	性别	男

单位名称	险种类型	起始年月	截止年月
中国移动通信集团河南有限公司	工伤保险	201710	-
中国移动通信集团河南有限公司	企业职工基本养老保险	201707	-
中国移动通信集团河南有限公司南阳分公司	失业保险	201709	-

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	2017-07-01	参保缴费	2017-09-01	参保缴费	2017-10-21	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	11507	●	11507	●	11507	-
02	11507	●	11507	●	11507	-
03	11507	●	11507	●	11507	-
04	11507	●	11507	●	11507	-
05	11507	●	11507	●	11507	-
06	11507	●	11507	●	11507	-
07	12253	●	12253	●	12253	-
08	12253	●	12253	●	12253	-
09	12253	●	12253	●	12253	-
10	12253	●	12253	●	12253	-
11	12253	●	12253	●	12253	-
12	12253	●	12253	△	12253	-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，○表示外地转入，-表示未制定计划。

4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

河南省社会保险中心 业务查询专用章

打印时间：2023-12-14

公共资源交易平台技防专用 AE2C15...C7764...1162...8BC...14DB9

4.10 移动—高锋杰—云应用集成交付工程师证书及社保证明



编号 HUC230310000122
Serial Number

TRAINING CERTIFICATE

工程师培训证书

本证书授予
This is to certify that Mr./Ms.

高锋杰

自 From 2022/06/13 至 to 2022/06/17 完成以下培训
completed the training program for

云应用集成交付工程师中级认证培训

该项目包含如下课程
The training program includes

课程名称（Courses）

业务系统安装部署与持续集成

云应用集成交付工程师中级结课考试

华为全球培训中心
Huawei Global Training Center

HUAWEI

2022/06/17
签发日期
Date of Issue

表单验证号码34d70e9493a045e89ce921be3af58cfc

河南省社会保险个人参保证明

（ 2023 年）

单位：元

证件类型	居民身份证	证件号码	411303198605150O1X		
社会保障号码	411303198605150O1X	姓　名	高锋杰	性别	男

单位名称	险种类型	起始年月	截止年月
河南百硕商务服务有限公司	工伤保险	201510	201508
中国移动通信集团河南有限公司	企业职工基本养老保险	200910	-
河南百硕商务服务有限公司	失业保险	200910	201508
中国移动通信集团河南有限公司	工伤保险	201803	-
河南百硕商务服务有限公司	企业职工基本养老保险	200910	201508
河南百硕商务服务有限公司	工伤保险	200910	201508
中国移动通信集团河南有限公司南阳分公司	失业保险	201802	-
中国移动通信集团河南有限公司郑州分公司	失业保险	201510	201801

缴费明细情况

月份	基本养老保险		失业保险		工伤保险	
	参保时间	缴费状态	参保时间	缴费状态	参保时间	缴费状态
	2009-10-01	参保缴费	2018-02-01	参保缴费	2009-10-19	参保缴费
	缴费基数	缴费情况	缴费基数	缴费情况	缴费基数	缴费情况
01	11015	●	11015	●	11015	-
02	11015	●	11015	●	11015	-
03	11015	●	11015	●	11015	-
04	11015	●	11015	●	11015	-
05	11015	●	11015	●	11015	-
06	11015	●	11015	●	11015	-
07	11239	●	11239	●	11239	-
08	11239	●	11239	●	11239	-
09	11239	●	11239	●	11239	-
10	11239	●	11239	●	11239	-
11	11239	●	11239	●	11239	-
12	11239	●	11239	△	11239	-

说明：

1、本证明的信息，仅证明参保情况及在本年内缴费情况，本证明自打印之日起三个月内有效。

2、扫描二维码验证表单真伪。

3、●表示已经实缴，△表示欠费，○表示外地转入，-表示未制定计划。

4、工伤保险个人不缴费，如果工伤保险基数正常显示，-表示正常参保。

5、若参保对象存在在多个单位参保时，以参加养老保险所在单位为准。

河南省社会保险中心 业务查询专用章

公共资源交易平台技术专用

4.11 华为—姚鹏—云服务解决方案架构师及社保证明



HUAWEI

Huawei Certification

Yao Peng

has successfully completed the Huawei certification requirements and is recognized as a

Cloud Service

Solutions Architect

HCIP

Cloud Service

Valid Through Sep 13, 2026

Validate this certificate's authenticity at
https://e.huawei.com/cn/talent/#/cert/certificate-verification
Certificate No. 01020260219380925061140 9

© Huawei Technologies Co. , Ltd. and/or its affiliate

CEO
Huawei Technologies Co., Ltd.



华为

华为认证

姚鹏

已顺利完成华为认证要求，并被公认为

云服务

解决方案架构师

Hsawei认证

HCIP

云服务

有效期至2026年9月13日

验证此证书的真实性
https://e.huawei.com/cn/talent/#/证书/证书验证
证号010202602193809250611409

©华为技术有限公司及/或其关联公司

首席执行官
华为技术有限公司

公共资源交易平台投标专用
AE2C19CEC776A6E1462A8BC58EA14DB9

注：华为认证证书英文转中文如图所示，其余同类证书不再一一翻译

江苏省社会保险权益记录单（参保单位）

参保单位全称： 华为云计算技术有限公司南京分公司　　**现参保地：** 雨花台区

统一社会信用代码： 91320114MA27AA21XU　　**查询时间：** 202212-202311

序号	姓名	公民身份号码（社会保障号）	缴费起止年月	缴费月数
1	姚鹏	41020219[illegible]263079[illegible]	202212 - 202311	12

说明：
1. 本权益单涉及单位及参保职工个人信息，单位应妥善保管。
2. 本权益单为打印时参保情况。
3. 本权益单已签具电子印章，不再加盖鲜章。
4. 本权益单记录单出具后有效期内（6个月），如需核对真伪，请使用江苏智慧人社APP，扫描右上方二维码进行验证（可多次验证）。

打印时间：2023年12月20日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

4.12 华为—王春光—云服务解决方案架构师及社保证明



HUAWEI

Huawei Certification

Chunguang Wang

has successfully completed the Huawei certification requirements and is recognized as a

Cloud Service

Solutions Architect

HCIP

Cloud Service

Valid Through Oct 10, 2026

Validate this certificate's authenticity at
https://e.huawei.com/cn/talent/#/cert/certificate-verification
Certificate No. 0102026021938092544921844444

© Huawei Technologies Co. , Ltd. and/or its affiliates

CEO
Huawei Technologies Co., Ltd.

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

北京市社会保险个人权益记录(单位职工缴费信息)

社会保险登记号:91110108MA04G0LJ7A　　校验码：kwc5rd

统一社会信用代码(组织机构代码):91110108MA04G0LJ7A　　查询流水号：1101082023121817532 4

单位名称:北京华为云计算技术有限公司　　查询日期：2022年12月至2023年12月

序号	姓名	社会保障号码	险种	缴费情况		本单位实际缴费月数
				起始年月	截止年月	
1	王春光	412826198806224612	养老保险	2022年12月	2023年11月	12
			失业保险	2022年12月	2023年11月	12
			工伤保险	2022年12月	2023年11月	12
			医疗保险	2022年12月	2023年11月	12
			生育保险	2022年12月	2023年11月	12

备注：

1.如需鉴定真伪，请30日内通过登录 http://fuwu.rsj.beijing.gov.cn/bjdkhy/ggfw/，进入“社保权益单校验”，录入校验码和查询流水号进行甄别，黑色与红色印章效力相同。

2.为保证信息安全，请妥善保管个人权益记录。

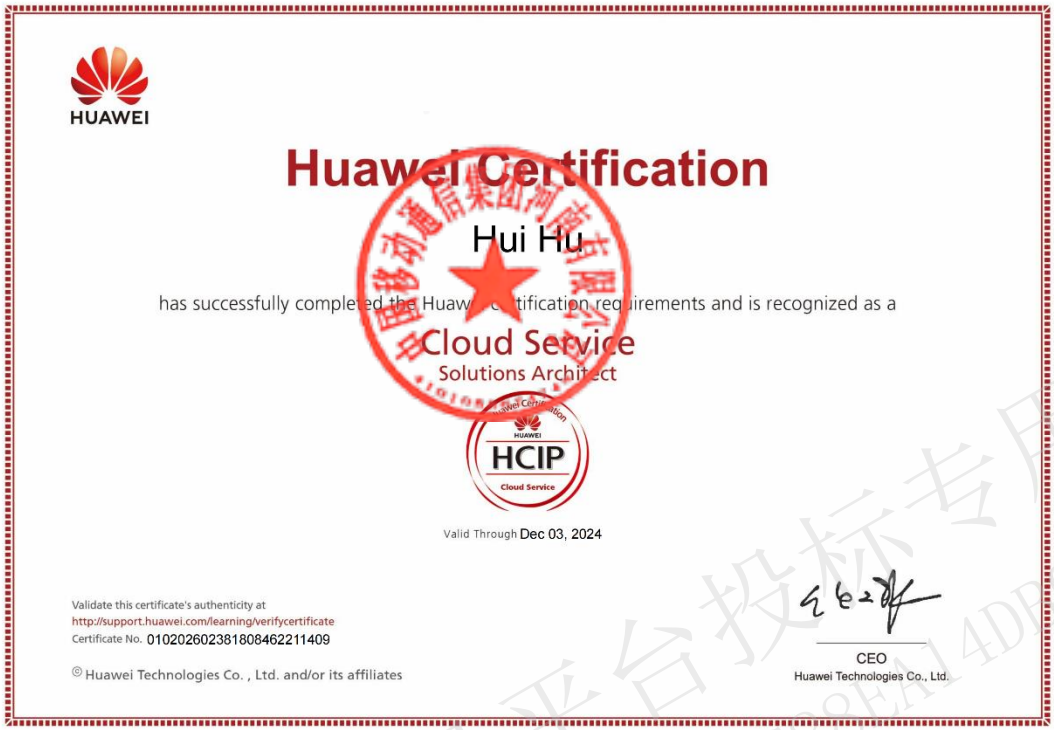
3.养老、工伤、失业保险相关数据来源于社保经办机构，医疗、生育保险相关数据来源于医保经办机构。

北京市海淀区社会保险基金管理中心

日期:2023年12月18日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

4.13 华为—胡辉—云服务解决方案架构师及社保证明



HUAWEI

Huawei Certification

Hui Hu

has successfully completed the Huawei certification requirements and is recognized as a

Cloud Service
Solutions Architect

HCIP
Cloud Service

Valid Through Dec 03, 2024

Validate this certificate's authenticity at
http://support.huawei.com/learning/verifycertificate
Certificate No. 01020260238180846221 1409

© Huawei Technologies Co., Ltd. and/or its affiliates

CEO
Huawei Technologies Co., Ltd.

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

北京市社会保险个人权益记录(单位职工缴费信息)

社会保险登记号:91110108802001707X7　　校验码：hb048u

统一社会信用代码(组织机构代码):91110108802001707X7　　查询流水号：1101082023121817454 8

单位名称:华为技术有限公司北京研究所　　查询日期：2022年12月至2023年12月

序号	姓名	社会保障号码	险种	缴费情况		本单位实际缴费月数
				起始年月	截止年月	
1	胡辉	510225197406263696	养老保险	2022年12月	2023年11月	12
			失业保险	2022年12月	2023年11月	12
			工伤保险	2022年12月	2023年11月	12
			医疗保险	2022年12月	2023年11月	12
			生育保险	2022年12月	2023年11月	12

备注：

1.如需鉴定真伪，请30日内通过登录 http://fuwu.rsj.beijing.gov.cn/bjdkhy/ggfw/，进入“社保权益单校验”，录入校验码和查询流水号进行甄别，黑色与红色印章效力相同。

2.为保证信息安全，请妥善保管个人权益记录。

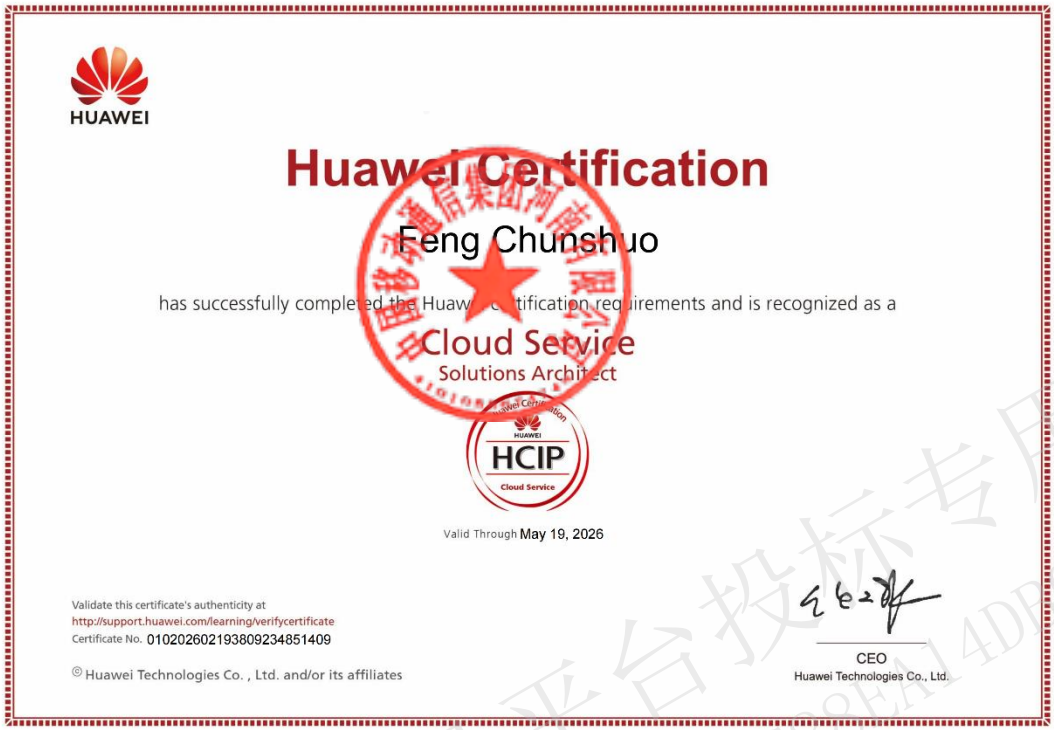
3.养老、工伤、失业保险相关数据来源于社保经办机构，医疗、生育保险相关数据来源于医保经办机构。

北京市海淀区社会保险基金管理中心

日期：2023年12月18日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

4.14 华为—冯纯硕—云服务解决方案架构师及社保证明



HUAWEI

Huawei Certification

Feng Chunshuo

has successfully completed the Huawei certification requirements and is recognized as a

Cloud Service
Solutions Architect

HCIP
Cloud Service

Valid Through May 19, 2026

Validate this certificate's authenticity at
http://support.huawei.com/learning/verifycertificate
Certificate No. 01020260219380923485 1409

© Huawei Technologies Co., Ltd. and/or its affiliates

CEO
Huawei Technologies Co., Ltd.

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

河南省城镇职工企业养老保险在职职工信息查询单

单位编号 412001100716　　业务年度：202312　　单位：元

单位名称	华为安驰智行技术有限公司				
姓名	冯纯硕	个人编号	41019990405813	证件号码	411081198802114571
性别	男	民族	汉族	出生日期	1988-02-11
参加工作时间	2013-09-10	参保缴费时间	2013-09-01	建立个人账户时间	2013-09
内部编号		缴费状态	参保缴费	截止计息年月	2022-12

个人账户信息

缴费时间段	单位缴费划转账户		个人缴费划转账户		账户本息	账户累计月数	重复账户月数
	本金	利息	本金	利息			
201309-202212	[redacted]					77	0
202301-至今						12	0
合计						89	0

[illegible]息

欠费月数	[redacted]	重复欠费月数	[redacted]	单位欠费金额	[redacted]	个人欠费本金	[redacted]	欠费本金合计	[redacted]

个人历年缴费基数

1992年	1993年	1994年	1995年	1996年	1997年	1998年	1999年	2000年	2001年
2002年	2003年	2004年	2005年	2006年	2007年	2008年	2009年	2010年	2011年
2012年	2013年	2014年	2015年	2016年	2017年	2018年	2019年	2020年	2021年
	[redacted]								
2022年	2023年								
[redacted]									

个人历年各月缴费情况

年度	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	年度	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1992													1993									▲	●	●	●
1994										▲	▲	▲	1995	▲	▲	▲	▲	▲	●	▲	▲	▲	▲	●	●
1996	▲	●	●	●	▲	●	▲	▲	●	▲	●	●	1997	●	●	●	●	●	●	●	●	●	●	●	●
1998	●	●	●	●	●	●	▲	●	●	●	●		1999												
2000													2001									▲	●	●	●
2002													2003									▲	●	●	●
2004													2005									▲	●	●	●
2006													2007									▲	●	●	●
2008													2009									▲	●	●	●
2010													2011									▲	●	●	●
2012													2013									▲	●	●	●
2014	●	●	●	●	●	●				▲	▲	▲	2015	▲	▲	▲	▲	▲	●	▲	▲	▲	▲	●	●
2016	▲	●	●	●	▲	●	▲	▲	●	▲	●	●	2017	●	●	●	●	●	●	●	●	●	●	●	●
2018	●	●	●	●	●	●	▲	●	●	●	●		2019												
2020													2021									▲	●	●	●
2022	●	●	●	●	●	●	●	●	●	●	●	●	2023	●	●	●	●	●	●	●	●	●	●	●	●

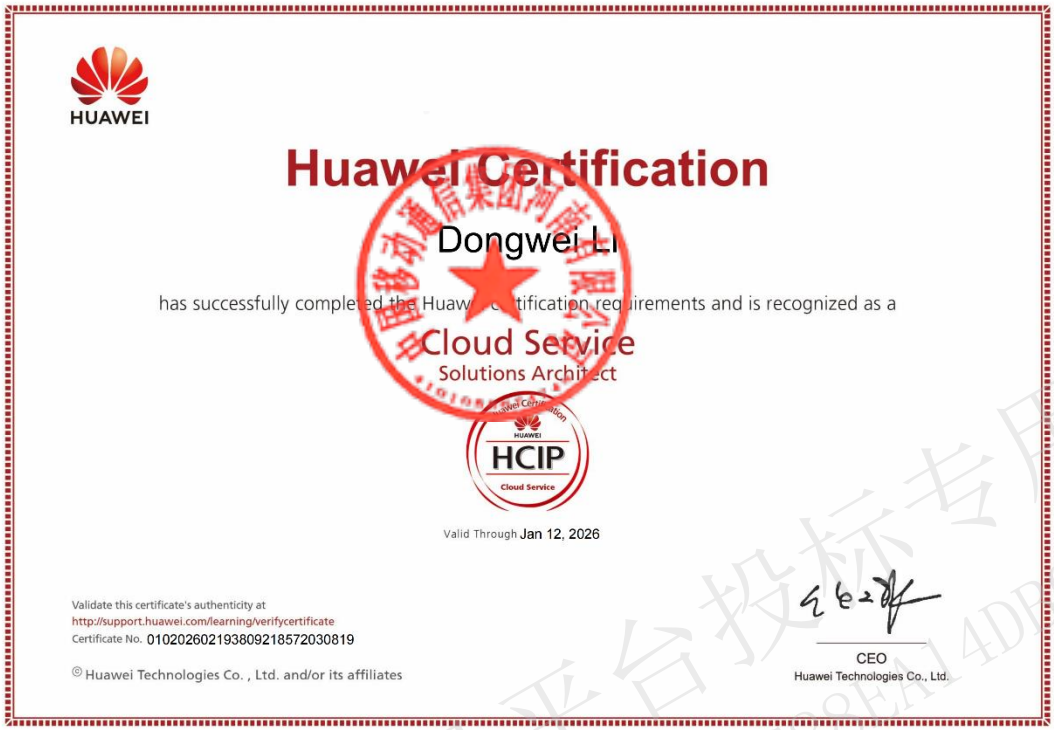
说明：“△”表示欠费、“▲”表示补缴、“●”表示当月缴费、“□”表示调入前外地转入。

人员基本信息为当前人员参保情况，个人账户信息、欠费信息、个人历年缴费基数、个人历年各月缴费情况查询范围为全省。如显示有重复缴费月数或重复欠费月数，说明您在多地存在重复参保。该表单黑白印章具有同等法律效力,可通过微信等第三方软件扫描单据上的二维码,查验单据的真伪。

打印日期：2023-12-18

公示信息仅供个人查询使用 AE2C19CE0

4.15 华为—李东伟—云服务解决方案架构师及社保证明



HUAWEI

Huawei Certification

Dongwei Li

has successfully completed the Huawei certification requirements and is recognized as a

Cloud Service
Solutions Architect

HCIP
Cloud Service

Valid Through Jan 12, 2026

Validate this certificate's authenticity at
http://support.huawei.com/learning/verifycertificate
Certificate No. 0102026021938092185720308l9

© Huawei Technologies Co., Ltd. and/or its affiliates

CEO
Huawei Technologies Co., Ltd.

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

验证码：8jpapv3wqj

西安高新技术产业开发区社会保险基金管理中

Xi'an Hi-tech Industries Development Zone Social Insurance Fund Office

西安高新技术产业开发区

社会保险参保缴费情况证明

西安华为技术有限公司：

兹证明参保单位：西安华为技术有限公司，在我中心参加养老、失业、工伤等社会保险，目前缴费正常，参保人员名单见附页。

特此证明。

西安高新区社会保险基金管理中心

（签章）

2023年12月18日

需特殊说明事项：　　（无）

说明：本《参保缴费证明》由参保单位根据需要在“西安高新区社会保险网上服务大厅”相应模块中选择打印，可作为参保人在我区参加社会保险的证明。本证明采用电子验证方式，不再加盖红色公章。证明使用单位可通过左上角的验证码登录我中心网页进行核验，验证码有效期：2024年3月18日之前（有效期内验证码可多次使用），验证网址：https://61.185.220.174:7316/（点击“材料验真”验证）。验证码请妥善保管，慎防泄漏。

地址：西安高新区锦业路1号 都市之门A座610室 邮编：710065

电话：029-88333626　　传真：029-88333866

第1页/共2页

公共资源交易平台 仅供专用

西安高新技术产业开发区社会保险基金管理中

Xi'an Hi-tech Industries Development Zone Social Insurance Fund Office

职工社会保险参保缴费人员名单

单位名称： 西安华为技术有限公司 单位编号： 850480

序号	姓名	身份证号码	户口性质	参保险种			备注
				养老	失业	工伤	
1	李东伟	411123198209264511	城镇	有	有	有	

注：1、"有"表示此险种正常参保，"无"表示此险种未参保。

2、参保人员缴费时间为三年内的，"备注"栏会注明开始缴费月份；缴费时间在三年以上的，"备注"栏不再特别标注。

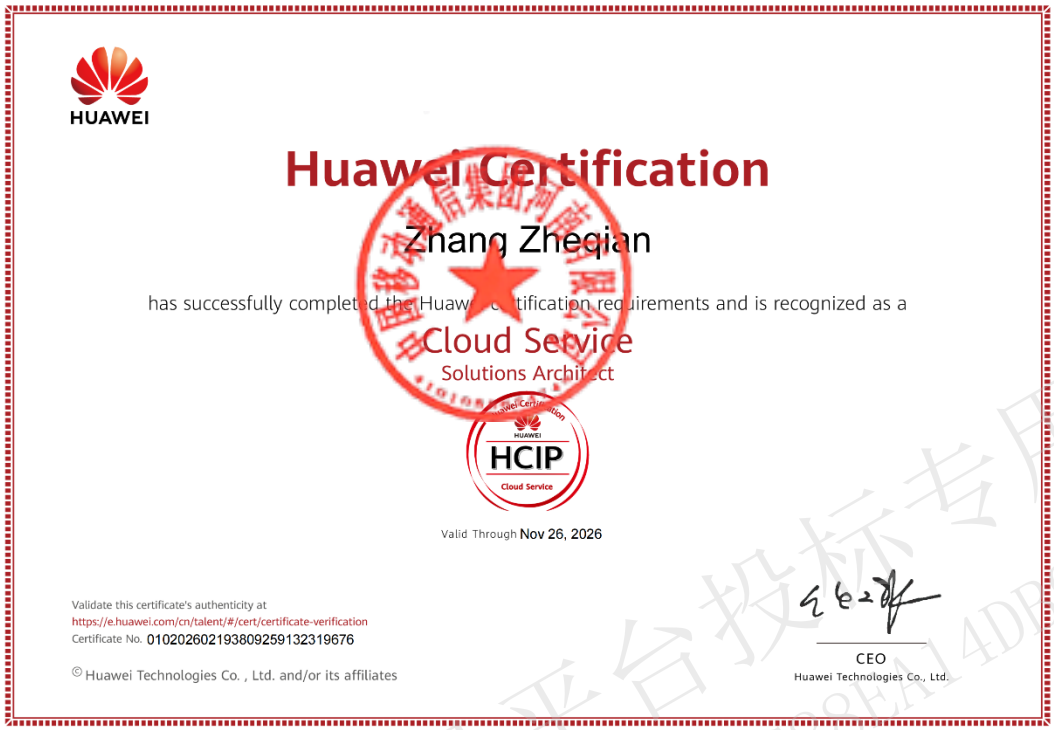
西安高新区社会保险基金管理中心

(签章)

2023年12月18日

公共资源交易平台招标专用
AE2C19CEC77646E1A62A8

4.16 华为—张哲千—云服务解决方案架构师及社保证明



HUAWEI

Huawei Certification

Zhang Zheqian

has successfully completed the Huawei certification requirements and is recognized as a

Cloud Service

Solutions Architect

HCIP

Cloud Service

Valid Through Nov 26, 2026

Validate this certificate's authenticity at
https://e.huawei.com/cn/talent/#/cert/certificate-verification
Certificate No. 0102026021938092591323196 76

© Huawei Technologies Co. , Ltd. and/or its affiliates

CEO
Huawei Technologies Co., Ltd.

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC8 8EA14DB9

缴纳社会保险证明

兹证明华为技术有限公司为以下人员，自 2022 年 12 月至 2023 年 11 月已向深圳市社会保险基金管理局参加了各种社会保险，包括养老保险、医疗保险、工伤保险、失业保险及生育医疗保险（其中工伤保险可享受有因工伤残和死亡待遇）。

特此证明！

序号	姓名	参保身份证号	保险号
1	张哲千	370305199209190734	647375589

华为技术有限公司

人事部

二〇二三年十二月十九日

公共资源交易平台投标专用
AE2C19CEC77[illegible]E1A62A8BC88EA14DB9

五、技术偏差表

项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目　　项目编号：南阳政采公开-2023-111

序号	名称	招标文件要求	投标文件功能	偏离	说明
1	计算-云主机	提供 VCPU 及内存	我方提供 VCPU 及内存	无偏离	
2	计算-云主机 GPU 基础版）	1、提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不 低于 128bits。 （直通型） 2、提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不 低于 128bits。 （虚拟化）	1、我方提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不低于 128bits。 （直通型） 2、我方提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G GDDR6 显存、位宽不低于 128bits。（虚拟化）	无偏离	
3	计算-云主机（GPU 标准版）	1、提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*2 GDDR6 显存、位宽 不低于 128bits。 （直通型） 2、提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*2 GDDR6 显存、位宽 不低于 128bits。 （虚拟化） 3、提供 V100 卡或同档显卡，提 供高性能图形计算加速，提供 不低于 32G*1 显存、位宽不低于 256bits。 （直通型） 4、提供 V100 卡或同档显卡，提 供高性能图	1、我方提供 T4 卡或同档显卡，提供高性能图形计算加速，我方提供不低于 16G*2 GDDR6 显存、位宽不低于 128bits。 （直通型） 2、我方提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G*2 GDDR6 显存、位宽不低于 128bits。 （虚拟化） 3、我方提供 V100 卡或同档显卡，提供高性能图形计算加速，我方提供不低于 32G*1 显存、位宽不低于 256bits。 （直通型） 4、我方提供 V100 卡或同档显卡，提供高性能图形	无偏离	

公共资源交易平台

		形计算加速，提供 不低于 32G*1 显存、位宽不低于 256bits。 （虚拟化）	计算加速，提供不低于 32G*1 显存、位宽不低于 256bits。 （虚拟化）		
4	计算-云主机（GPU 高级版）	1、提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*4 GDDR6 显存、位宽 不低于 128bits。 （直通型） 2、提供 T4 卡或同档显卡，提供 高性能图形计算加速，提供不 低于 16G*4 GDDR6 显存、位宽 不低于 128bits。 （虚拟化） 3、提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G*2 显存、位宽不 低于 256bits。 （直通型） 4、提供 V100 卡或同档显卡，提 供高性能图形计算加速，提供 不低于 32G*2 显存、位宽不低于 256bits。 （虚拟化）	1、我方提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G*4 GDDR6 显存、位宽不低于 128bits。 （直通型） 2、我方提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16G*4 GDDR6 显存、位宽不低于 128bits。 （虚拟化） 3、我方提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G*2 显存、位宽不低于 256bits。 （直通型） 4、我方提供 V100 卡或同档显卡，提供高性能图形计算加速，提供不低于 32G*2 显存、位宽不低于 256bits。 （虚拟化）	无偏离	
5	计算-物理机（计算型）	1、2 路： 单 CPU>=10 核， Mem>=64G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=128G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=192G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=256G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=384G,本地硬盘(SAS 盘)>=600G*2	1、2 路： 单 CPU>=10 核， Mem>=64G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=128G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=192G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=256G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=384G,本地硬盘(SAS 盘)>=600G*2	无偏离	

公共资源交易平台投标专用
AE2C19CEC7764CF1A82A8BC8214DB9

		单 CPU>=10 核， Mem>=512G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=128G,本地硬盘(SAS 盘)>=600G*2 2、4 路： 单 CPU>=10 核， Mem>=192G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=256G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=512G,本地硬盘(SAS 盘)>=600G*2	单 CPU>=10 核， Mem>=512G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=128G,本地硬盘(SAS 盘)>=600G*2 2、4 路： 单 CPU>=10 核， Mem>=192G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=256G,本地硬盘(SAS 盘)>=600G*2 单 CPU>=10 核， Mem>=512G,本地硬盘(SAS 盘)>=600G*2		
6	计算-GPU 卡	1、物理机叠加，单卡提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16GGDDR6 显存、显存位宽不低于 256bits。 2、物理机叠加，单卡提供 V100 卡或同档显卡，提供高性能图 形计算加速，提供不低于 32G 显存，位宽不低于 256bits。	1、物理机叠加，单卡提供 T4 卡或同档显卡，提供高性能图形计算加速，提供不低于 16GGDDR6 显存、显存位宽不低于 256bits。 2、物理机叠加，单卡提供 V100 卡或同档显卡，提供高性能图 形计算加速，提供不低于 32G 显存，位宽不低于 256bits。	无偏离	
7	操作系统	1、Linux Server：根据需要提供合适的版本（包括国产操作系统） 2、Windows Server：根据需要提供合适的版本	1、Linux Server：根据需要提供合适的版本（包括国产操作系统） 2、Windows Server：根据需要提供合适的版本	无偏离	
8	存储-低 IO	低 IO: 适用于云硬盘、文件存储、对象存储，介质为 SATA,HDD，30MB/s<吞吐量<40MB/s，100<IOPS<1000。	低 IO: 适用于云硬盘、文件存储、对象存储，介质为 SATA,HDD，30MB/s<吞吐量<40MB/s，100<IOPS<1000。	无偏离	

公共资源交易平台技术规范
AE2C19CEC776481162A8BC8

9	存储-中 IO	中 IO: 适用于云硬盘，介质为 SAS 盘 HDD，40MB/s<吞吐量 140MB/s，1000<IOPS<5000	中 IO: 适用于云硬盘，介质为 SAS 盘 HDD，40MB/s<吞吐量 140MB/s，1000<IOPS<5000	无偏离	
10	存储-高 IO	高 IO： 适用于云硬盘，介质为 SSD 盘，140MB/s<吞吐量<300MB/s，5000<IOPS<25000	高 IO： 适用于云硬盘，介质为 SSD 盘，140MB/s<吞吐量<300MB/s，5000<IOPS<25000	无偏离	
11	存储-视频存储	提供视频存储	我方提供视频存储	无偏离	
12	存储-共享存储	适用于共享云硬盘，具备多挂 载点、高并发性、高性能、高 可靠性等特点。主要应用于需要支持集群、HA（High Available，指高可用集群）能力的关键企业应用场景，多个云服务器可同时访问一个共享云硬盘，FC-SAN 存储空间，介质为 SAS 盘 HDD	适用于共享云硬盘，具备多挂载点、高并发性、高性能、高 可靠性等特点。主要应用于需要支持集群、HA（High Available，指高可用集群）能力的关键企业应用场景，多个云服务器可同时访问一个共享云硬盘，FC-SAN 存储空间，介质为 SAS 盘 HDD	无偏离	
13	数据备份-虚拟机/文件备份	支持本地备份、异地备份（定时）	支持本地备份、异地备份（定时）	无偏离	
14	数据备份-数据库备份	支持本地备份、异地备份（定时）	支持本地备份、异地备份（定时）	无偏离	
15	虚拟负载均衡	提供负载均衡	我方提供负载均衡	无偏离	

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA140B9

16	云数据库-关系型数据库	1、提供稳定可靠、可弹性伸缩的 在线数据库服务，是一种高安 全、高可用，易运维的 MySQL 数据库，提供备份、恢复、监 控服务等基本功能，配合提供数据库基础运维服务，需搭配 块存储使用，存储另行计费。 2、关系型数据库 Oracle，提供安装与激活服务，提供数据库 基础运维服务。 3、SQL Server 拥有高可用架构和数据恢复功能，包含 License 授权，支持实例管理、账号管理、数据库管理、 白名单、备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存 储另行计费。 4、缓存数据库 Redis，提供数据 监控、数据管理、数据安全、 备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存储另行计费。集群版： 主从版*2 5、关系型数据库 PostgreSQL， 配合提供数据库基础运维服	1、提供稳定可靠、可弹性伸缩的 在线数据库服务，是一种高安全、高可用，易运维的 MySQL 数据库，提供备份、恢复、监 控服务等基本功能，配合提供数据库基础运维服务，需搭配 块存储使用，存储另行计费。 2、关系型数据库 Oracle，提供安装与激活服务，提供数据库 基础运维服务。 3、SQL Server 拥有高可用架构和数据恢复功能，包含 License 授权，支持实例管理、账号管理、数据库管理、 白名单、备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存 储另行计费。 4、缓存数据库 Redis，提供数据 监控、数据管理、数据安全、 备份恢复等基本功能，配合提供数据库基础运维服务，需搭配块存储使用，存储另行计费。集群版： 主从版*2 5、关系型数据库 PostgreSQL， 配合提供数据库基础运维服	无偏离	
17	云数据库-分布式关系型数据库	基于普通服务器和横向扩展 的方式，构建支持海量数据存 储和访问的数据库系统，从而实现无线扩容和弹性扩展。	基于普通服务器和横向扩展 的方式，构建支持海量数据存 储和访问的数据库系统，从而实现无线扩容和弹性扩展。	无偏离	
18	云数据库-分布式文档数据库	基于分布式文档数据库，提供 稳定可靠、可弹性伸缩的在线 数据库服务，是一种高安全、 高可用，易运维的数据库，提 供备份、恢复、监控服务等基 本功能，配合提供数据库基础运维服务。	基于分布式文档数据库，提供 稳定可靠、可弹性伸缩的在线 数据库服务，是一种高安全、 高可用，易运维的数据库，提 供备份、恢复、监控服务等基本功能，配合提供数据库基础运维服务。	无偏离	

公共资源交易平台技术专用
AE2C19CEC7154E0A9E5C8

19	云数据库-国产数据库	提供不少于三种国产数据库， 提供租用、安装、调优、排错、技术支持。	我方提供不少于三种国产数据库， 提供租用、安装、调优、排错、技术支持。	无偏离	
20	大数据服务-实时计算	提供流式计算引擎，将各种不同的数据源中的数据进行实 时的订阅、处理、分析。	我方提供流式计算引擎，将各种不同的数据源中的数据进行实 时的订阅、处理、分析。	无偏离	
21	大数据服务-离线计算	服务于批量结构化数据的存 储和计算，可以提供海量数据 仓库的解决方案,存储另算。	服务于批量结构化数据的存 储和计算，可以提供海量数据 仓库的解决方案,存储另算。	无偏离	
22	大数据服务-搜索引擎	提供数据分析、搜索等场景服 务,存储另算。	我方提供数据分析、搜索等场景服务,存储另算。	无偏离	
23	大数据服务-分析计算	提供对海量数据进行即时的 多维分析透视和业务探索，快速构建数据仓库,存储另算。	我方提供对海量数据进行即时的 多维分析透视和业务探索，快速构建数据仓库,存储另算。	无偏离	
24	容器服务	根据部署容器的节点数按月计费（仅包括节点管理费用，不包含资源费用，云服务器/云服务器_Disk/负载均衡/EIP/专有网络等资源另行计算）	根据部署容器的节点数按月计费（仅包括节点管理费用，不包含资源费用，云服务器/云服务器_Disk/负载均衡/EIP/专有网络等资源另行计算）	无偏离	
25	应用服务-应用与数据集成服务	提供将物联网、大数据、视频、统一通信、GIS 等基础平台及各个应用的服务、消息、数据统一集成适配以及编排的能力。	我方提供将物联网、大数据、视频、统一通信、GIS 等基础平台及各个应用的服务、消息、数据统一集成适配以及编排的能力。	无偏离	
26	应用服务-应用管理	应用管理平台，提供资源及业务应用的实时监控、实时告警事件、统一日志收集和分析等功能。	应用管理平台，提供资源及业务应用的实时监控、实时告警事件、统一日志收集和分析等功能。	无偏离	
27	应用服务-应用工厂服务	应用管理与运维平台为开发人员、测试人员、运维人员或项目经理等角色，提供应用托管、监控、告警和日志分析等能力提供以应用为中心的应用发布、部署、监控、告警、日志等一站式管理能力。	应用管理与运维平台为开发人员、测试人员、运维人员或项目经理等角色，提供应用托管、监控、告警和日志分析等能力提供以应用为中心的应用发布、部署、监控、告警、日志等一站式管理能力。	无偏离	

公共资源交易平台提供支持
AE2C19CEC77646E

28	应用服务-应用迁移	系统迁移服务	系统迁移服务	无偏离	
29	网络及托管服务-互联网带宽	提供互联网访问独享带宽 2-100Mbps 部分，每 2 兆带宽 40 元，超过 100M 部分，每 2 兆带宽 34 元）	我方提供互联网访问独享带宽 2-100Mbps 部分，每 2 兆带宽 40 元，超过 100M 部分，每 2 兆带宽 34 元）	无偏离	
30	网络及托管服务-互联网 IP	提供互联网 IP 地址，IPv4 版（IPv6 地址免费）	我方提供互联网 IP 地址，IPv4 版（IPv6 地址免费）	无偏离	
31	网络及托管服务-设备托管	1、提供 1U 托管机位 2、提供 42U 标准托管机架（3.5KW）	1、提供 1U 托管机位 2、提供 42U 标准托管机架（3.5KW）	无偏离	
32	云桌面	提供云桌面授权，不含终端，支持软拨号。	我方提供云桌面授权，不含终端，支持软拨号。	无偏离	
33	云安全-虚拟防火墙	提供虚拟网络安全区域边界安全防护能力。	我方提供虚拟网络安全区域边界安全防护能力。	无偏离	
34	云安全-虚拟漏洞扫描	提供虚拟化漏洞扫描功能，包含数据库漏洞扫描、系统漏洞扫描、WEB 漏洞扫描、主机基线配置核查、网络基线配置核查等功能模块，提供报告。	我方提供虚拟化漏洞扫描功能，包含数据库漏洞扫描、系统漏洞扫描、WEB 漏洞扫描、主机基线配置核查、网络基线配置核查等功能模块，提供报告。	无偏离	
35	云安全-虚拟堡垒机	提供虚拟化运维安全管理与审计系统(堡垒机)安全能力	我方提供虚拟化运维安全管理与审计系统(堡垒机)安全能力	无偏离	
36	云安全-虚拟主机安全	虚拟机形态部署，提供资产管理、安全体检、安全监控、漏洞风险、入侵威胁、合规基线等多个功能模块，各个模块进行联动，模块间数据联通，形成闭环系统，为企业提供强有力的采集、检测、监测、防御、捕获能力，对主机进行全方位的安全防护。	虚拟机形态部署，提供资产管理、安全体检、安全监控、漏洞风险、入侵威胁、合规基线等多个功能模块，各个模块进行联动，模块间数据联通，形成闭环系统，为企业提供强有力的采集、检测、监测、防御、捕获能力，对主机进行全方位的安全防护。	无偏离	

公共资源交易平台技术专用
AE2C19CEC

37	云安全-虚拟Web 应用防火墙	提供虚拟化 WAF 安全能力。	我方提供虚拟化 WAF 安全能力。	无偏离	
38	云安全-网页防篡改	提供网页防篡改功能。	我方提供网页防篡改功能。	无偏离	
39	云安全-虚拟日志审计	提供日志分析系统，支持日志的采集、过滤、归并、关联分析、展现、告警监控、实施事件监控、报表等。	我方提供日志分析系统，支持日志的采集、过滤、归并、关联分析、展现、告警监控、实施事件监控、报表等。	无偏离	
40	云安全-虚拟VPN 安全接入	提供国密 SSLVPN 加密服务，移动办公安全接入，包括接入用户身份认证、传输数据加密、权限划分和接入审计，每 100 个 VPN 并发组件。	我方提供国密 SSLVPN 加密服务，移动办公安全接入，包括接入用户身份认证、传输数据加密、权限划分和接入审计，每 100 个 VPN 并发组件。	无偏离	
41	云安全-虚拟防病毒	提供虚拟化防病毒能力。	我方提供虚拟化防病毒能力。	无偏离	
42	云安全-入侵检测	整机吞吐量≧10Gbps。	整机吞吐量≧10Gbps。	无偏离	
43	云安全-虚拟数据库审计	针对用户对数据库的访问行为进行记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源。加强内外部数据库网络行为记录，提高数据资产安全。	针对用户对数据库的访问行为进行记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源。加强内外部数据库网络行为记录，提高数据资产安全。	无偏离	
44	云安全-虚拟密码机	能够为政务云提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，可以满足通用密码服务，保证传输信息的机密性、完整性和有效性，司时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。	能够为政务云提供高性能的、多任务并行处理的密码运算，支持 SM1、SM2、SM3、SM4 等多种国产密码算法，可以满足通用密码服务，保证传输信息的机密性、完整性和有效性，司时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。	无偏离	

公共资源交易中心共享云用
AE2C19CEC

45	云安全-数据库加密服务	200 实例。	200 实例。	无偏离	
46	总体要求	本技术要求参照《关于发布<国家电子政务外网信息安全标准体系框架>等七项安全标准的通知》（政务外网〔2014〕11 号）、《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55 号）、《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》（国办函〔2016〕108 号）等文件制定。 本技术要求是基本要求，投标人可进行优化，具体响应方案中的功能性能可优于本技术要求。 （1）投标人须承诺配合采购人做好政务云监管平台接入及政务云安全工作，确保本项目达到国家监管部门要求。 （2）投标人承诺在签订合同后按工期完成云服务平台安装部署，并具备服务能力。 （3）投标人须承诺无条件做好各单位业务应用迁移上云工作。 （4）投标人须承诺未经允许不得对云平台上的任何数据进行截取、加工、分析和处理，或提供给第三方。 （5）投标人须承诺在服务期结束后，无条件配合各使用单位迁移应用系统，提供服务退出承诺书。	本技术要求参照《关于发布<国家电子政务外网信息安全标准体系框架>等七项安全标准的通知》（政务外网〔2014〕11 号）、《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55 号）、《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》（国办函〔2016〕108 号）等文件制定。 本技术要求是基本要求，投标人可进行优化，具体响应方案中的功能性能可优于本技术要求。 （1）我方承诺配合采购人做好政务云监管平台接入及政务云安全工作，确保本项目达到国家监管部门要求。 （2）我方在签订合同后按工期完成云服务平台安装部署，并具备服务能力。 （3）我方承诺无条件做好各单位业务应用迁移上云工作。 （4）我方承诺未经允许不得对云平台上的任何数据进行截取、加工、分析和处理，或提供给第三方。 （5）我方承诺在服务期结束后，无条件配合各使用单位迁移应用系统，提供服务退出承诺书。 （6）机房要求：提供云平台需要的机房环境，包含安全可控的独立机房区域、电力、机柜、制冷、门禁及视频监控等，标准不低于国标 B 级。 （7）云管理平台要求：通过云管理平台软件对资源	无偏离	详见 3.10 对技术要求的承诺书

公共资源交易平台投标专用
AE2C19CEC7764[illegible]

		（6）机房要求：提供云平台需要的机房环境，包含安全可控的独立机房区域、电力、机柜、制冷、门禁及视频监控等，标准不低于国标 B 级。 （7）云管理平台要求：通过云管理平台软件对资源进行管理，提供弹性计算、自动化部署、资源区域划分等功能，通过统一的接口为云运营平台和云监管平台提供相关功能要求。 （9）基础安全要求：符合《信息安全技术 云计算服务安全指南》(GB/T31167-2014)、《信息安全技术 网络安全等级保护实施指南》(GB/T25058-2019)、《信息系统密码应用基本要求》(GM/T0054-2018)等规范要求，政务云平台应通过信息安全等级保护三级认证、商用密码应用安全性评估、云计算服务安全评估。政务云平台应在不同层面保障政务云安全，包括基础设施安全、云平台安全、云租户安全、平台运维安全、平台合规审计等，并提供网络隔离、租户隔离、漏洞扫描、主机安全、日志审计、通用密码、数据库加密等安全及密码能力。 采购的云计算服务，相关网络安全部分，如果未有明确要求，按上级政策规定执行。 （10）网络要求：提供 SDN、VxLAN 相关网络服务，支持与互联网、电子政务外网及行业部门专网的连接。提供与电子政务外网核心交换	进行管理，提供弹性计算、自动化部署、资源区域划分等功能，通过统一的接口为云运营平台和云监管平台提供相关功能要求。 （9）基础安全要求：符合《信息安全技术 云计算服务安全指南》(GB/T31167-2014)、《信息安全技术 网络安全等级保护实施指南》(GB/T25058-2019)、《信息系统密码应用基本要求》(GM/T0054-2018)等规范要求，政务云平台应通过信息安全等级保护三级认证、商用密码应用安全性评估、云计算服务安全评估。政务云平台应在不同层面保障政务云安全，包括基础设施安全、云平台安全、云租户安全、平台运维安全、平台合规审计等，并提供网络隔离、租户隔离、漏洞扫描、主机安全、日志审计、通用密码、数据库加密等安全及密码能力。 采购的云计算服务，相关网络安全部分，如果未有明确要求，按上级政策规定执行。 （10）网络要求：提供 SDN、VxLAN 相关网络服务，支持与互联网、电子政务外网及行业部门专网的连接。提供与电子政务外网核心交换节点连接的专线。 （11）我方按照采购人要求，提供详细的技术实施方案。 （12）配合各政务部门使用政务云或者迁移应用系统至政务云平台等相关工作，投标人主要负责但不限于如下工作： 1）配合各单位应用系统迁移前的环境需求分析工		

公共资源交易平台 AE2C19CEC7

		节点连接的专线。 （11）投标人必须按照采购人要求，提供详细的技术实施方案。 （12）配合各政务部门使用政务云或者迁移应用系统至政务云平台等相关工作，投标人主要负责但不限于如下工作： 1）配合各单位应用系统迁移前的环境需求分析工作。 2）负责各单位应用系统迁移前的测试环境搭建工作。 3）配置物理服务器、配置虚拟机、配置网络、安装操作系统、配置相应的安全策略等。 4）配合或提供各单位应用系统迁移需要使用的迁移工具。 5）配合各单位应用系统迁移过程中遇到问题故障分析以及提出解决方案，并配合解决问题故障。 6）负责各单位应用系统迁移过程中对硬件、网络、软件、安全等运行环境的变更工作。 7）配合各单位应用系统迁移后进行测试工作，如压力测试、故障测试等。	作。 2）负责各单位应用系统迁移前的测试环境搭建工作。 3）配置物理服务器、配置虚拟机、配置网络、安装操作系统、配置相应的安全策略等。 4）配合或提供各单位应用系统迁移需要使用的迁移工具。 5）配合各单位应用系统迁移过程中遇到问题故障分析以及提出解决方案，并配合解决问题故障。 6）负责各单位应用系统迁移过程中对硬件、网络、软件、安全等运行环境的变更工作。 7）配合各单位应用系统迁移后进行测试工作，如压力测试、故障测试等。		
47	机房	机房空间要求满足本期摆放空间，并具备后期扩展能力	我方机房空间满足本期摆放空间，并具备后期扩展能力	无偏离	
48	传输线路	提供 2 路及以上传输线路	我方提供 2 路及以上传输线路	无偏离	

公共资源交易平台投标专用
AE2C19CEC77646E1A62ABBC88EA14DB9

49	云管理平台	提供云服务器生命周期管理包括镜像与磁盘管理、安全组，提供云平台操作截图证明。 提供云服务器 CPU 和内存状态监控功能，监控内容包括不限于 24 小时的 CPU 利用率趋势图、内存使用率趋势，提供云平台操作截图证明；提供云服务器网络监控功能，监控内容包括网络流入带宽、网络流出带宽，提供云平台操作截图证明； 所使用的云平台支持云服务器快照功能，提供云平台操作截图证明。 所使用的云平台支持短信、邮件告警通知，提供云平台操作截图证明。	提供云服务器生命周期管理包括镜像与磁盘管理、安全组，提供云平台操作截图证明。 提供云服务器 CPU 和内存状态监控功能，监控内容包括不限于 24 小时的 CPU 利用率趋势图、内存使用率趋势，提供云平台操作截图证明；提供云服务器网络监控功能，监控内容包括网络流入带宽、网络流出带宽，提供云平台操作截图证明； 所使用的云平台支持云服务器快照功能，提供云平台操作截图证明。 所使用的云平台支持短信、邮件告警通知，提供云平台操作截图证明。	无偏离	详见 9.10 对技术要求的截图证明或证明材料
50	计算资源池	云主机（ECS）可用性≥99.99%，提供相关证明材料。	云主机（ECS）可用性≥99.99%，提供相关证明材料。	无偏离	详见 9.10 对技术要求的截图证明或证明材料
51	存储资源池	块存储（云硬盘）和对象存储数据存储持久性≥ 99.9999%，提供提供相关证明材料。	块存储（云硬盘）和对象存储数据存储持久性≥ 99.9999%，提供提供相关证明材料。	无偏离	详见 9.10 对技术要求的截图证明或证明材料
52	网络资源池	提供满足要求的网络资源池能力	我方提供满足要求的网络资源池能力	无偏离	
53	安全资源池	提供满足要求的虚拟化安全能力	我方提供满足要求的虚拟化安全能力	无偏离	

公共资源交易平台投标专用
AE2C19CEC[illegible]CFE1A62[illegible]8C88EA14DB9

54	云数据库	云数据库业务可用性满足基本要求且≥99.99%，云数据库的数据存储持久性≥99.9999%,提供相关证明材料。	云数据库业务可用性满足基本要求且≥99.99%，云数据库的数据存储持久性≥99.9999%,提供相关证明材料。	无偏离	详见9.10 对技术要求的截图证明或证明材料
55	监管接口	提供满足云监管平台和统一安全运维所需的接口	我方提供满足云监管平台和统一安全运维所需的接口	无偏离	
56	运维要求	提供满足政务云标准要求的运维服务方案	我方提供满足政务云标准要求的运维服务方案	无偏离	
57	故障处理	提供满足政务云标准要求的故障处理方案	我方提供满足政务云标准要求的故障处理方案	无偏离	
58	应急响应	提供满足政务云标准要求的应急响应方案	我方提供满足政务云标准要求的应急响应方案	无偏离	
59	信息安全保障服务	提供满足政务云标准要求的信息安全保障服务方案	我方提供满足政务云标准要求的信息安全保障服务方案	无偏离	
60	租户安全	安全部分应满足租户安全需要，保证政务业务系统的网络安全、数据安全等。	安全部分应满足租户安全需要，保证政务业务系统的网络安全、数据安全等。	无偏离	

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

61	运维要求	投标人需提供素质高、专业性强、经验丰富、稳定的运维团队，主要负责整个政务云平台的软硬件和网络运维。投标人需要为本项目选派专业技术人员参与本项目实施运维，需运维人员至少 8 名，包括云核心技术提供方的原厂或原厂授权运维人员至少 3 名、其他运维人员至少 5 名。投标人需有严格的、有组织、有纪律的管理运维流程，并指派专职联络员，团队需要 7×24 小时在岗及时响应故障请求，负责云平台的故障受理、处理、跟踪、结果汇报工作。 为保证云平台服务可用性及运行效率，供应商云平台的服务能力须保证各个应用系统可用性不低于 99.99%；供应商云资源交付响应时间不超过 2 个工作日。 运维方案应从整运维服务体系的宗旨、运维服务体系架构、运维服务体系的内容、运维管理制度、人员培训等方面来阐述说明。	我方提供素质高、专业性强、经验丰富、稳定的运维团队，主要负责整个政务云平台的软硬件和网络运维。投标人需要为本项目选派专业技术人员参与本项目实施运维，需运维人员至少 8 名，包括云核心技术提供方的原厂或原厂授权运维人员至少 3 名、其他运维人员至少 5 名。投标人需有严格的、有组织、有纪律的管理运维流程，并指派专职联络员，团队需要 7×24 小时在岗及时响应故障请求，负责云平台的故障受理、处理、跟踪、结果汇报工作。 为保证云平台服务可用性及运行效率，供应商云平台的服务能力须保证各个应用系统可用性不低于 99.99%；供应商云资源交付响应时间不超过 2 个工作日。 运维方案应从整运维服务体系的宗旨、运维服务体系架构、运维服务体系的内容、运维管理制度、人员培训等方面来阐述说明。	无偏离	
62	故障处理	投标人必须承诺在签订合同后，实行 7×24 小时运行维护和响应故障工作，负责政务云平台的故障受理、处理、跟踪、结果汇报工作。切实保障政务云平台基础环境的安全、稳定、高效的运行。 对于一般故障要求投标人 30 分钟内进行响应；对于重大故障要求 10 分钟内进行响应；对于特别重大故障要求 5 分钟内进行响应。	我方承诺在签订合同后，实行 7×24 小时运行维护和响应故障工作，负责政务云平台的故障受理、处理、跟踪、结果汇报工作。切实保障政务云平台基础环境的安全、稳定、高效的运行。 对于一般故障要求投标人 30 分钟内进行响应；对于重大故障要求 10 分钟内进行响应；对于特别重大故障要求 5 分钟内进行响应。 故障处理方案应从故障处理的流程、网络故障处	无偏离	

公共资源交易平台 AE2C19CEC7

		故障处理方案应从故障处理的流程、网络故障处理、服务器故障处理、业务系统故障处理等方面来阐述说明。	理、服务器故障处理、业务系统故障处理等方面来阐述说明。		
63	应急响应	投标人应提供系统故障应急处理预案，提供出现问题的快速解决方法，制定完善合理的应急响应方案。 投标人每年应进行不少于 2 次的应急演练。 应急响应方案应从响应时间、电力应急、空调应急、消防应急、网络及系统应急、云平台故障应急等方面来阐述说明。	我方提供系统故障应急处理预案，提供出现问题的快速解决方法，制定完善合理的应急响应方案。 每年应进行 2 次的应急演练。 应急响应方案应从响应时间、电力应急、空调应急、消防应急、网络及系统应急、云平台故障应急等方面来阐述说明。	无偏离	
64	信息安全保障服务	投标人应遵循国家电子政务信息安全保障体系要求，参考国家主管部门发布的相关标准规范要求，提供明确、完善、可行的安全建设方案，充分考虑在网络、系统、数据库、应用等方面的安全性。 投标人须从机房、网络、安全、虚拟机、物理机、存储、运维等方面加强信息安全管理，避免因出现问题引起信息安全责任事故。 信息安全保障服务方案应从保障措施、预防措施、风险评估、质量保障等方面来阐述说明。	我方遵循国家电子政务信息安全保障体系要求，参考国家主管部门发布的相关标准规范要求，提供明确、完善、可行的安全建设方案，充分考虑在网络、系统、数据库、应用等方面的安全性。 须从机房、网络、安全、虚拟机、物理机、存储、运维等方面加强信息安全管理，避免因出现问题引起信息安全责任事故。 信息安全保障服务方案应从保障措施、预防措施、风险评估、质量保障等方面来阐述说明。	无偏离	

投标人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间：2023 年 12 月 22 日

六、商务偏差表

商务偏差表

项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目

项目编号：南阳政采公开-2023-111

序号	招标文件商务条款	投标文件商务	偏差描述	结论
1	投标邀请函->三、采购内容及要求： 1、项目概况：根据南阳市政府关于政务云平台建设的相关要求，南阳市政务服务和大数据管理局组织进行政务云服务采购。政务云主要为全市各政务部门提供高性能物理机、云主机、云存储、云应用、云安全和异地备份等基础设施资源共享服务，为各政务部门间数据交换、共享、应用等提供基础平台支撑。本项目服务对象是党政机关、事业单位等。 2、服务期限：3 年。	采购内容及要求： 1、项目概况：根据南阳市政府关于政务云平台建设的相关要求，南阳市政务服务和大数据管理局组织进行政务云服务采购。政务云主要为全市各政务部门提供高性能物理机、云主机、云存储、云应用、云安全和异地备份等基础设施资源共享服务，为各政务部门间数据交换、共享、应用等提供基础平台支撑。本项目服务对象是党政机关、事业单位等。 2、服务期限：3 年。	无偏差	
2	投标邀请函->四、项目预算：云服务总预算 4500 万元/3 年，每年预算 1500 万元，含 91 项服务项和云租户安全两部分，其中 91 项服务项单价之和不得大于 74088 元/月，服务能力 11000 基础运算单元（vcpu、内存），同时每个单项均不得超过该项最高服务限价；云租户安全部分不得超过 180 万/年。	我公司项目报价：云服务总报价小于 4500 万元/3 年，每年报价小于 1500 万元，含 91 项服务项和云租户安全两部分，其中 91 项服务项单价之和小于 74088 元/月，服务能力 11000 基础运算单元（vcpu、内存），同时每个单项均不得超过该项最高服务限价；云租户安全部分小于 180 万/年。	无偏差	
3	投标邀请函->十三、投标人具备的条件 1、投标人须是注册于中华人民共和国境内的企业法人或负责人或其他组织，具有有效的统一社会信用代码的营业执照；	我公司是注册于中华人民共和国境内的企业，具有有效的统一社会信用代码的营业执照	无偏差	

4	投标邀请函->十三、投标人具备的条件 2、具有良好的商业信誉和健全的财务会计制度；	我公司具有良好的商业信誉和健全的财务会计制度；	无偏差	
5	投标邀请函->十三、投标人具备的条件 3、具有履行合同所必需的设备和专业技术能力	我公司具有履行合同所必需的设备和专业技术能力	无偏差	
6	投标邀请函->十三、投标人具备的条件 4、有依法缴纳税收和社会保障资金的良好记录	我公司有依法缴纳税收和社会保障资金的良好记录	无偏差	
7	投标邀请函->十三、投标人具备的条件 5、2020 年以来在经营活动中没有重大违法记录；	我公司 2020 年以来在经营活动中没有重大违法记录，提供承诺函	无偏差	
8	投标邀请函->十三、投标人具备的条件 6、遵守国家有关法律、法规、规章；	我公司遵守国家有关法律、法规、规章；	无偏差	
9	投标邀请函->十三、投标人具备的条件 7、本项目不接受联合体投标；	我公司独立参加本项目投标，非联合体投标；	无偏差	
10	投标邀请函->十三、投标人具备的条件 8、根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》(财库[2016]125 号)的规定，对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，拒绝参与本项目政府采购活动【查询渠道：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）】，查询时间为发布公告之日起到投标截止时间。	我公司提供失信被执行人、重大税收违法案件当事人、政府采购严重违法失信行为记录查询截图，【查询渠道：“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）】，查询时间为发布公告之日起到投标截止时间。	无偏差	
11	项目商务要求->1、投标人应提供本项目技术方案、应急保障服务能力方案、运维人员名单及基本情况等。	我公司提供本项目技术方案、应急保障服务能力方案、运维人员名单及基本情况等。	无偏差	

公共资源交易平台投标专用

12	项目商务要求->2、根据上级文件要求，进行国产化改造、建设、替代、迁移，须在投标文件中提供承诺书。	根据上级文件要求，进行国产化改造、建设、替代、迁移，须在投标文件中提供承诺书。	无偏差	
13	项目商务要求->3、本项目服务质量：合格，符合现行国家相关验收规范标准，达到采购人满意。	本项目服务质量：合格，符合现行国家相关验收规范标准，达到采购人满意。	无偏差	
14	项目商务要求->4、投标人必须具备独立完成本项目的能力，中标后不允许分包、转包。	我公司具备独立完成本项目的能力，中标后不允许分包、转包。	无偏差	
15	项目商务要求->5、合同的签订：中标供应商自行打印电子营业执照系统中加盖南阳市政府采购中心签章的《中标通知书》后，及时与采购人签订服务合同。	合同的签订：如中标，我公司自行打印电子营业执照系统中加盖南阳市政府采购中心签章的《中标通知书》后，及时与采购人签订服务合同。	无偏差	
16	项目商务要求->6、中标人在签订合同之日起 15 日历天内，须按照招投标文件、合同要求完成政务云服务能力建设、系统安全建设、租户安全建设、运维团队组建等，达到招投标文件和合同的要求，符合验收条件。	如中标，我公司在签订合同之日起 15 日历天内，按照招投标文件、合同要求完成政务云服务能力建设、系统安全建设、租户安全建设、运维团队组建等，达到招投标文件和合同的要求，符合验收条件。	无偏差	
17	项目商务要求->7、合同履行期限：合同签订之日起至 3 年服务期结束。	合同履行期限：合同签订之日起至 3 年服务期结束。	无偏差	
18	项目商务要求->8、项目验收：采购人在合同签订后 15 日历天依据国家、省市相关规定和招投标文件、合同进行验收。主要包括服务能力验收、技术验收（性能、功能、信息安全等）、资料验收（主要包括建设方案、信息安全相关报告、政务云符合性测评报告、功能安全测试报告、系统安全性评估报告、机房图纸、运维方案等）。验收方式包括通过现场查阅资料、软件演示、现场测试、质询等进行。 验收期间，服务项中基础运算单元（vcpu、内存）不得低于采购预算单元的 50%，安全产品全部到位。	项目验收：采购人在合同签订后 15 日历天依据国家、省市相关规定和招投标文件、合同进行验收。主要包括服务能力验收、技术验收（性能、功能、信息安全等）、资料验收（主要包括建设方案、信息安全相关报告、政务云符合性测评报告、功能安全测试报告、系统安全性评估报告、机房图纸、运维方案等）。验收方式包括通过现场查阅资料、软件演示、现场测试、质询等进行。 验收期间，服务项中基础运算单元（vcpu、内存）不得低于采购预算单元的 50%，安全产品全部到位。	无偏差	

19	项目商务要求->9、付款方式：按照《河南省政务云管理办法》第二十四条要求，依据云服务目录据实结算。验收合格后，服务费用按年度结算。	付款方式：按照《河南省政务云管理办法》第二十四条要求，依据云服务目录据实结算。验收合格后，服务费用按年度结算。	无偏差	
20	投标人须知表->投标有效期：60日历日	投标有效期：60日历日	无偏差	
21	投标人须知表->投标文件制作要求： 1、投标人须提供电子投标文件一一份。 2、投标人应按照本招标文件中第五部分--投标文件格式的要求制作投标文件。如有漏项或采购中心、采购人认为其投标文件有明显缺陷的，造成的后果由投标人自己承担。 3、电子投标文件应使用企业电子营业执照生成并在截止时间前上传其加密版本，具体详见《电子营业执照应用平台系统操作手册-投标单位》。否则，被视为无效投标文件，将被电子营业执照应用平台系统拒绝。 4、电子投标文件需使用“电子营业执照应用平台投标文件制作工具（南阳版）”生成。电子投标文件中的图片应清晰可辩，否则所导致的一切后果由投标人自行承担。 5、投标文件文字：投标文件均以中文印制，中文以外的文字应附以中文译文，中外文不符时以中文为准。 6、投标文件计量单位：除在招标文件的技术规格中有规定的之外，计量单位使用中华人民共和国法定计量单位。 7、投标人编制投标文件时，涉及营业执照、资质、业绩、财务、社保、纳税及各类证书、报告等内容，必须是原件的扫描件。	投标文件制作要求： 1、我公司提供电子投标文件一一份。 2、我公司按照本招标文件中第五部分--投标文件格式的要求制作投标文件。如有漏项或采购中心、采购人认为其投标文件有明显缺陷的，造成的后果由我公司自己承担。 3、电子投标文件应使用企业电子营业执照生成并在截止时间前上传其加密版本，具体详见《电子营业执照应用平台系统操作手册-投标单位》。否则，被视为无效投标文件，将被电子营业执照应用平台系统拒绝。 4、电子投标文件需使用“电子营业执照应用平台投标文件制作工具（南阳版）”生成。电子投标文件中的图片应清晰可辩，否则所导致的一切后果由投标人自行承担。 5、投标文件文字：投标文件均以中文印制，中文以外的文字应附以中文译文，中外文不符时以中文为准。 6、投标文件计量单位：除在招标文件的技术规格中有规定的之外，计量单位使用中华人民共和国法定计量单位。 7、我方编制投标文件时，涉及营业执照、资质、业绩、财务、社保、纳税及各类证书、报告等内容，都是原件的扫描件。	无偏差	

公共资源交易平台 电子投标专用

22	无采购人不能接受的附加条件	我方投标文件未含有采购人不能接受的附加条件。	无偏差	
23	其他	招标文件中要求的其他全部商务条款我公司均完全响应	无偏差	

投标人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

七、投标人业绩

7.1 安阳市政务服务和大数据管理局安阳市政务云平台服务采购项目

7.1.1 中标公告



2023/12/7 16:54 安阳市政府采购网

您好，欢迎访问安阳市政府采购网！ 服务热线：0371-65808207

安阳市政府采购网
Government Procurement Of Anyang

输入关键字，搜索相关信息

首页 工作动态 通知公告 采购信息 购买服务 监督管理 政策法规 政策解读 操作指南 文件下载 公众咨询

安阳市政务服务和大数据管理局安阳市政务云平台服务采购项目-成交公告

发布机构：安阳市政府采购中心 发布日期：2023-06-27 10:09 访问次数：5804

中小微企业融资申请

一、项目基本情况

1、采购项目编号：安财单一采购-2023-4

2、采购项目名称：安阳市政务服务和大数据管理局安阳市政务云平台服务采购项目

3、采购方式：单一来源

4、采购公告发布日期：2023年06月14日

5、评审日期：2023年06月26日

二、成交情况

包号	采购内容	供应商名称	地 址	中标金额	单位
安财单一采购-2023-4	安阳市政务服务和大数据管理局安阳市政务云平台服务采购	中国移动通信集团河南有限公司安阳分公司	安阳市文峰区中华路中段	22,879,713.60	元

序号	名称	服务范围	服务要求	服务时间	服务标准
1	安阳市政务服务和大数据管理局安阳市政务云平台服务采购	详见单一来源文件	详见单一来源文件	3年	详见单一来源文件

三、评审专家名单

赵紫刚、李劲松、杜国真、戴晶磊、任帅（采购人代表）

四、代理服务收费标准及金额

收费标准：无

收费金额：0.00元

本项目相关公告

安阳市政务服务和大数管理局安阳市政务云平

安阳市政务服务和大数管理局安阳市政务云平

安阳市政务服务和大数

本项目进度

合同 2023-07-27

www.hngp.gov.cn/anyang/content?infold=1420551&channelCode=H660202 1/2

公共资源交易平台投标专用

五、成交公告发布的媒介及成交公告期限

本次中标公告在《河南省政府采购网》《安阳市公共资源交易中心网》上发布，成交公告期限为1个工作日 。

六、其他补充事宜

无

七、凡对本次公告内容提出询问，请按以下方式联系

1. 采购人信息

名称：安阳市政务服务和大数据管理局

地址：安阳市文峰区文峰大道东段市民之家七楼

联系人：任帅

联系方式：13673803533

2.采购代理机构信息（如有）

名称：安阳市政府采购中心

地址：安阳市文峰大道东段559号市民之家四楼

联系人：樊敬琨

联系方式：0372-3397792

3.项目联系方式

项目联系人：任帅

联系方式：13673803533

附件

安阳市政务服务和大数据管理局安阳市政务云平台服务采购.doc

版权所有 ©2007 河南省财政厅 网站标识码：4100000057 备案号：豫ICP备09005258号 豫公网安备 41010502004654号
地址：河南省郑州市经三路25号 邮编：450008 技术服务电话：0371-65808207、0371-65808480
今日本站访问人数：71425，今日本站访问量：102128，今日全站访问量：6520169，累计全站访问量：22801983140

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC38EA14DB9

7.1.2 中标通知书原件扫描件

安阳市政务服务和大数据管理局安阳市政务云平台服务采购项目成交通知书

中国移动通信集团河南有限公司安阳分公司：

我们荣幸的通知，贵方在采购编号为安财单一采购-2023-4安阳市政务服务和大数据管理局安阳市政务云平台服务采购项目采购中，您单位以贰仟贰佰捌拾柒万玖仟柒佰壹拾叁元陆角（22879713.6元）为成交供应商。

请贵单位根据单一来源采购文件、响应文件等，于本通知书发出之日起2个工作日内与安阳市政务服务和大数据管理局签订书面合同。

采购人要在合同签订之日起1个工作日内在“安阳市政府采购网”进行合同备案及公告。

安阳市政府采购中心

二〇二三年六月二十七日

温馨提示：

根据豫财购〔2017〕10号和安财购〔2017〕7号文件要求，参加政府采购项目的中小微企业供应商，持中标（成交）通知书可向金融机构申请合同融资。详情请登录安阳市政府采购网（http://www.hngp.gov.cn/anyang），进入网站飘窗或业务指南窗口了解金融机构提供的融资服务内容。

公共资源交易平台投标专用
AE2C15CEC77646E1A62A3BC88E14DB9

7.1.3 项目合同原件扫描件

合同编号：安财单一采购-2023-4

安阳市政务服务平台服务合同

甲方（盖章）：安阳市政务服务和大数据管理局

法定代表人或授权代表签字：

地址：安阳市市民之家7楼

乙方（盖章）：中国移动通信集团河南有限公司安阳分公司

法定代表人或授权代表签字：

地址：安阳市文明大道809号

合同签订日期：【2023】年【7】月【13】日

合同签订地点：【安阳市文峰大道市民之家7楼】

1

河南移动 合同管理
公共资源交易平台 投标专用
AE2C13CEC1F6461...2A8BC88EA14DB9
扫描全能王

按照 2023 年 6 月 27 日签发的《安阳市政务服务和大数据管理局安阳市政务云平台服务采购项目中标通知书》，根据《中华人民共和国民法典》及相关法律法规和招、投标文件，双方就安阳市政务云平台服务采购项目的有关事宜达成如下协议。

第一条　服务内容

乙方为甲方提供的服务内容包括：基础设施资源服务、软件支撑服务、安全服务。

1.1 基础设施资源服务

主机托管服务：提供机柜空间，租户存放自己的主机。

云主机服务：提供各类配置的云主机，满足业务的不同需求。

计算服务：提供负载均衡服务等。

网络接入服务：提供云专线，提供公网 IP。

云存储服务：提供不同形式的云存储空间。

1.2 软件支撑服务

操作系统服务：提供正版 Windows Server 和 Linux Server。

云备份服务：提供虚拟机备份、应用级备份服务等。

数据库服务：提供 MYSQL 数据库、SQL Server 数据库、IBM DB2 数据库、Oracle 数据库服务等。

中间件服务：提供消息队列、微服务等。

云安全服务：提供 WEB 防火墙、WEB 全栈防护服务等。

1.3 安全服务

密码安全服务：提供密码二级服务和密码三级服务。

第二条　服务要求

2.1 乙方所提供的服务应符合法律法规和国家、行业的相关标准，甲方的相关管理制度、标准或规范，乙方对甲方的各项承诺以及本合

公共资源交易平台合投标专用
AE2C19C5C7764C1A624B3C88EA14DB9
河南移动 合同管理
扫描全能王

同的要求。

2.2 乙方所提供服务的云管理系统应接入云计算指挥中心和市政务云资源管理监控系统，按照云服务相关政策和安阳市相关文件，每月提供资源使用情况报告，并配合甲方开展服务考核。

第三条　服务期限与地点

3.1 服务期限：自项目通过验收之日起三年。

3.2 服务地点：【河南省安[illegible]】。

第四条 双方权利义务

4.1 甲方有权对乙方提供的服务进行监督和检查。

4.2 甲方负责组织绩效考核，考核结果作为确定乙方履行情况的依据。

4.3 乙方负责提供招、投标文件中项目所需政务云的专业服务，须满足等保 2.0 三级和密码测评三级安全防护要求。

4.4 乙方负责提供运维支持、性能优化、技术咨询、定期巡检、技术培训等服务，每天对信息系统相关的各种设备与线路进行维护管理，提供 7*24 小时机房环境巡检和场与技术咨询服务。服务电话：18837250206。

乙方应委派一名具备国家法律法规要求的资质条件、身体健康并相对固定的专业技术人员提供驻场服务。若人员更换，需至少提前一周告知甲方并经甲方同意。

4.6 乙方进行检修线路、设备搬迁、工程割接、网络及软件升级或其他网络设备进行调试、维护工作，或因其他可预见性的原因可能影响甲方使用信息化服务的，应至少提前五个工作日通知甲方。

第五条　服务计费标准

扫描全能王

服务层次	服务分类	服务项	规格	单位	单价（元/月）
IaaS(基础设施服务)	主机托管	机柜空间（含电）	1U	U	202.35
		单个机柜	42U-44U（4kw）	个	3230
	云主机	云主机	两核+2GB	台	105.45
			两核+4GB	台	120.65
			两核+8GB	台	151.05
			两核+16GB	台	258.4
			四核+4GB	台	211.85
			四核+8GB	台	242.25
			四核+16GB	台	302.1
			四核+32GB	台	519.65
			八核+8GB	台	422.75
			八核+16GB	台	483.55
			八核+32GB	台	604.2
			八核+64GB	台	845.5
			十六核+16GB	台	845.5
			十六核+32GB	台	968.05
			十六核+64GB	台	1209.35
			三十二核+32GB	台	1691.95
			三十二核+64GB	台	1935.15
			三十二核+128GB	台	2417.75
		物理服务器租赁	CPU>=2 路 8 核 内存>=256G,本地硬盘>=600G	台	1054.5
			CPU>=2 路 10 核 内存>=320G,本地硬盘>=600G	台	1187.5
			CPU>=2 路 10 核 内存>=256G,本地硬盘>=6TB	台	1254
			CPU>=2 路 10 核 内存>=256G,本地硬盘>=6TB, SSD 硬盘>=1.92TB	台	1282.5
			CPU>=2 路 10 核,内存>=256G, 本地硬盘>=33.2TB, SSD 硬盘>=1.92TB	台	1748
			CPU>=2 路 14 核 内存>=320G,本地硬盘>=600G	台	1425
			CPU>=4 路 10 核 内	台	1900

河南移动 合同管理
中国移动通信集团河南有限公司
公共资源交易平台 仅供查看使用
AE2C19CEC77646E1A8BC5884A14DB9
扫描全能王

		存>=256G,本地硬盘>=600G		
		CPU>=4 路 14 核 内存>=320G,本地硬盘>=600G	台	2327.5
		CPU>=8 路 10 核 内存>=512G,本地硬盘>=600G	台	3325
		CPU>=8 路 14 核 内存>=512G,本地硬盘>=600G	台	4275
		CPU>=8 路 16 核 内存>=512G,本地硬盘>=600G	台	4655
计算	负载均衡	实例		11.4
网络接入	公网 IP	每云主机免费 1 个,超过按量收费	个	32.3
	互联网带宽	1G	Gbps	10093.75
云存储	SAN 存储	-	GB	0.22
	NAS 网络存储	-	GB	0.15
操作系统	Linux Server	实例(赠送 20GB 数据盘容量)	-	26.6
	Windows Server	实例(赠送 40GB 数据盘容量)	-	52.25
云备份	虚拟机备份	云主机配置和系统盘和数据盘备份	GB	0.11
	数据库备份		GB	0.11
	应用级备份		GB	0.4
数据库	MySQL 数据库	实例	1CPU	75.05
	SQL Server 数据库	实例	1CPU	202.35
	IBM DB2 数据库	企业版	1CPU	645.05
	Oracle 数据库	企业版	1CPU	753.35
中间件	消息队列微服务	两核	4GB	188.1
		四核	8GB	403.75
		八核	16GB	823.65
		十六核	32GB	1418.35
云安全	WEB 防火墙	集 WEB 防护、网页保护于一体的 WEB 整体安全防护设备的一款产品,提供虚拟化 WAF 安全能力	每 IP	214.7
	WEB 全栈防护	基于对 Web 流量的解码和分析,对恶意流量或攻击进	每 IP	428.45

扫描全能王

		行阻拦，从而保障 web 应用安全。		
密码安全服务	密码二级安全服务	提供含国密浏览器、国密 USBKey、国密 VPN 安全接入、国密数据加解密、国密签名验签服务；用户数量：用户<=50	-	1615
		提供含国密浏览器、国密 USBKey、国密 VPN 安全接入、国密数据加解密、国密签名验签服务；用户数量：50<用户<=100	-	3144.5
		提供含国密浏览器、国密 USBKey、国密 VPN 安全接入、国密数据加解密、国密签名验签服务；用户数量：100<用户<=500	-	8075
	密码三级安全服务	提供含国密浏览器、国密 USBKey、国密 VPN 安全接入、国密数据加解密、国密签名验签、国密电子签章、国密时间戳、国密手机盾签名认证服务；用户数量：用户<=50	-	2422.5
		提供含国密浏览器、国密 USBKey、国密 VPN 安全接入、国密数据加解密、国密签名验签、国密电子签章、国密时间戳、国密手机盾签名认证服务；用户数量：50<用户<=100	-	4845
		提供含国密浏览器、国密 USBKey、国密 VPN 安全接入、国密数据加解密、国密签名验签、国密电子签章、国密时间戳、国密手机盾签名认证服务；用户数量：100<用户<=500	-	8882.5

河南移动 合同管理
公共资源交易电子技术专用
AE2019CEC7764EB...C88A14DB9
扫描全能王

第六条 服务费用及付款方式

6.1 服务费用总价为：22879713.6 元，大写：贰仟贰佰捌拾柒万玖仟柒佰壹拾叁元陆角整。

6.2 服务费用从系统入驻政务云之日起算。后续甲方云主机扩容新增需求按照云服务资费的最优惠价执行。期间如乙方资费优惠下调，甲方按新资费优惠后价格执行。

6.3 服务资源实际使用量以[illegible]评审结果为准，服务费用根据考核结果据实结算。所有提供的服务均采用先使用后付费的方式。乙方承诺在每次付费前提供安阳市政务云平台当年有效期内的等保三级备案证书、三级商用密码应用安全[illegible]估报告和政务云风险评估报告。服务计费标准见本合同第五条。

6.4双方选择通过转账方式付款。

乙方银行收款账号：

乙方名称：【中国移动通信集团河南有限公司安阳分公司】

纳税人识别号：【91410500721816077T】

户名：【中国移动通信集团河南有限公司安阳分公司】

开户行：【中国工商银行安阳分行行政区支行】

账号：【1706 0201 2904 8092 394 】

联系电话：【0372-3305678 】

第七条 安全保障

7.1 乙方根据甲方需求，提供网络安全设备，用于网络安全防护。网络安全设备包括：防火墙、防病毒网关、IPS、IDS、WEB 网站防篡改系统、安全隔离及信息交换系统、漏洞扫描系统、综合日志审计系统、运维管理系统等内容，符合等保三级和商用密码三级测评要求。

7.2 网络安全策略由使用方负责制定，乙方负责实施，安全策略

公共资源交易平台投标专用

扫描全能王

配置完成后未经使用方书面授权，乙方不得单方面做出更改，由于乙方单方面行为导致网络故障、系统崩溃或数据丢失，由此造成的后果由乙方承担。

7.3 网络安全设备应保存至少六个月的运行日志，以便发生网络入侵时进行历史追溯。乙方应每周向甲方报送各网络安全设备的统计报表、防护日志等关键性日志信息，方便甲方及时掌握系统运行状况；

7.4 乙方应建立切实可行的网络安全应急预案，如遇突发性网络故障或网络安全威胁，乙方应立即启动应急预案，并第一时间告知甲方，由甲乙双方共同制定解决方案。

第八条 违约责任

8.1 任何一方不履行本合同约定的义务或履行义务不符合本合同约定的，均构成违约，应承担违约责任。

8.2 乙方未按照本合同的约定向甲方提供服务的，应承担违约责任：乙方在履行本合同时，不得对甲方的通信网络、信息网络发起任何形式的攻击、预留软件后门或内置黑客软件等，且乙方应当加强对其工作人员的工具、权限管理和教育，以避免前述攻击的发生。在发现乙方或乙方人员对甲方或甲方网管网络的前述攻击时，甲方将立即解除本合同，终止和乙方的任何合作，且乙方应当向甲方支付【10】万元的违约金，该违约金不足以弥补甲方损失的，不足部分，乙方应当赔偿。此处甲方的损失包括但不限于甲方处理由此引发的法律纠纷的全部费用等。

第九条 免责条款

1. 在执行合同期限内，任何一方因不可抗力事件所致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，以减轻可能给对方造

扫描全能王

成的损失，并应当在合理期限内提供发生不可抗力事件证明。

第十条　争议解决

1. 在本合同履行过程中发生争议，双方应当协商解决。

2. 双方协商不成，提交甲方所在地人民法院诉讼解决。

第十一条 合同生效、终止及其他

1. 本合同以中文签署，一式[illegible]份，甲方执叁份，乙方执叁份，具有相同法律效力。谈判文件、响应文件均为本合同的组成部分。

2. 合同变更和修改。合同的变更及修改须经双方同意，以书面形式变更，与本合同具有同等法律效力。

3. 本合同自双方法定代表人（负责人）或授权代表签字并盖章之日起生效；如双方签署日期不一致，自较迟的签署日起生效。

附件：绩效考核办法

河南移动 合同管理
河南移动 合同管理
河南移动 合同管理
公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

扫描全能王

7.2 濮阳市政府采购中心濮阳市政务信息系统迁移上云项目(二次)

7.2.1 中标公告



中国移动通信集团河南有限公司

濮阳市政府采购中心濮阳市政务信息系统迁移上云项目（二次）成交公告

发布机构：濮阳市政府采购中心　发布日期：2021-03-05 15:38　访问次数：12160

一、项目基本情况

1、采购项目编号：濮财市直磋商采购-2020-41

2、采购项目名称：濮阳市政府系统迁移上云

3、采购方式：竞争性磋商

4、采购公告发布日期：2021年02月09日

5、评审日期：2021年03月03日

二、成交情况

包号	采购内容	供应商名称	地址	中标金额	单位
濮财市直磋商采购-2020-41	濮阳市政府系统迁移上云	中国联合网络通信有限公司濮阳市分公司	濮阳市开州路与中原路交叉口	40.000	%
	序号	名称	服务范围	服务要求	服务时间	服务标准
	1	见附件	见附件	见附件	见附件	见附件
濮财市直磋商采购-2020-41	濮阳市政府系统迁移上云	中国电信集团有限公司河南分公司	郑州市金水东路29号	47.000	%
	序号	名称	服务范围	服务要求	服务时间	服务标准
	1	见附件	见附件	见附件	见附件	见附件
濮财市直磋商采购-2020-41	濮阳市政府系统迁移上云	中国移动通信集团河南有限公司濮阳分公司	濮阳市卫河北路36号	45.000	%
	序号	名称	服务范围	服务要求	服务时间	服务标准
	1	见附件	见附件	见附件	见附件	见附件

三、评审专家名单

宋海根、袁乾印、谢佳景、程雪生、罗伟（采购人代表）

本项目相关公告

濮阳市政府采购中心濮市政务信息系统迁移上成交公告

濮阳市政府采购中心濮市政务信息系统迁移上变更公告

本项目进度

采购公告 2021-0

开标

结果 2021-03-0

合同

公共资源交易平台投标专用
AE2C19CEC7646E1A62A8BC88EA14DB9

四、代理服务收费标准及金额

收费标准：本项目不收取代理服务费

收费金额：0.00元

五、成交公告发布的媒介及成交公告期限

本次中标公告在《河南省政府采购网》《中国政府采购网》《濮阳市政府采购网》《濮阳市公共资源交易平台》上发布。成交公告期限为1个工作日。2021年03月08日 至 2021年03月08日

六、其他补充事宜

1、评审情况表和中标单位的服务方案见附件 2、成交金额说明 中国联合网络通信有限公司濮阳市分公司：采购清单收费的40%；负责迁移35%的单位。 中国移动通信集团河南有限公司濮阳分公司：采购清单收费的45%；负责迁移33%的单位。 中国电信集团有限公司河南分公司：采购清单收费的47%；负责迁移32%的单位。

七、凡对本次公告内容提出询问，请按以下方式联系

1. 采购人信息

名称：濮阳市政务服务和大数据管理局

地址：濮阳市华龙区人民路158号

联系人：崔鹏

联系方式：13839380466

2.采购代理机构信息（如有）

名称：濮阳市政府采购中心

地址：濮阳市中原路和开州路交叉口向北50米路东濮阳市公共资源交易一楼

联系人：黄先生

联系方式：0393-8750928

3.项目联系方式

项目联系人：黄先生

联系方式：0393-8750928

附件

评审情况表.doc

联通-服务方案.docx

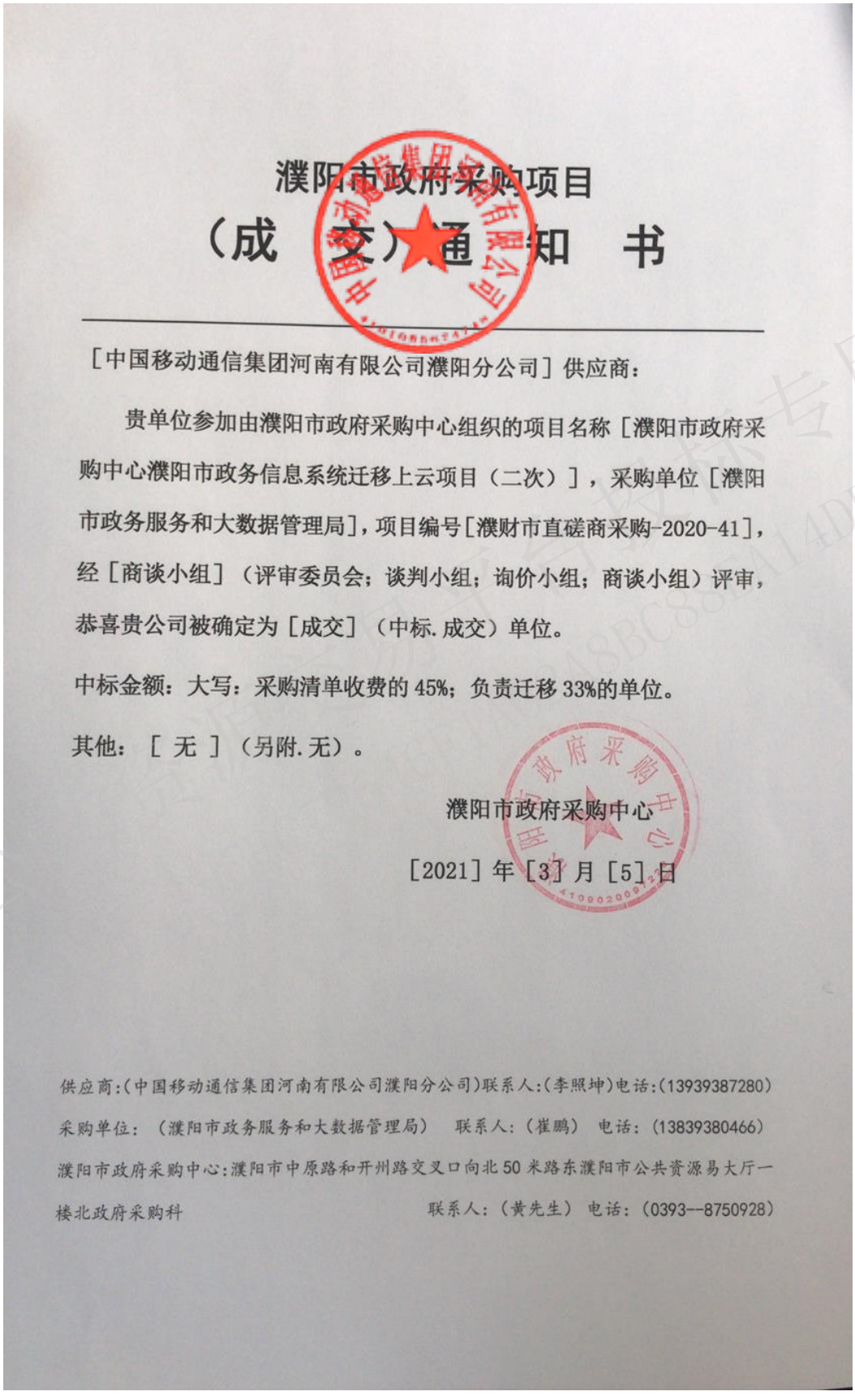
移动-服务方案.pdf

电信-服务方案.docx

公共资源交易平台投标专用
AE2C19C2E77646E1A62A8BC88EA14DB9

版权所有 ©2007 河南省财政厅 网站标识码：4100000057 备案号：豫ICP备09005258号 豫公网安备 41010502004654号
地址：河南省郑州市经三路25号 邮编：450008 技术服务电话：0371-65808207、0371-65808480
今日本站访问人数：112957，今日本站访问量：150981，今日全站访问量：11379155，累计全站访问量：10464637132

7.2.2 中标通知书原件扫描件



濮阳市政府采购项目

（成　交）通　知　书

[中国移动通信集团河南有限公司濮阳分公司] 供应商：

贵单位参加由濮阳市政府采购中心组织的项目名称 [濮阳市政府采购中心濮阳市政务信息系统迁移上云项目（二次）]，采购单位 [濮阳市政务服务和大数据管理局]，项目编号[濮财市直磋商采购-2020-41]，经 [商谈小组]（评审委员会；谈判小组；询价小组；商谈小组）评审，恭喜贵公司被确定为 [成交]（中标.成交）单位。

中标金额：大写：采购清单收费的45%；负责迁移33%的单位。

其他：[无]（另附.无）。

濮阳市政府采购中心

[2021] 年 [3] 月 [5] 日

供应商:(中国移动通信集团河南有限公司濮阳分公司)联系人:(李照坤)电话:(13939387280)

采购单位：（濮阳市政务服务和大数据管理局）　联系人:（崔鹏）　电话:（13839380466）

濮阳市政府采购中心:濮阳市中原路和开州路交叉口向北50米路东濮阳市公共资源易大厅一楼北政府采购科　联系人:（黄先生）　电话:（0393--8750928）

7.2.3 项目合同原件扫描件

【濮阳市政务服务和大数据管理局】与中国移动通信集团河南有限公司【濮阳】分公司政务云服务合作协议

甲方：【濮阳市政务服务和大数据管理局】（盖章）

法定代表人： 刘道光

地址：濮阳市人民路158号

授权代表签字：

乙方：【中国移动通信集团河南有限公司濮阳分公司】（盖章）

法定代表人： 虎威

地址：濮阳市卫河北路36号

授权代表签字：

合同签订日期：【 2022 】年【 12 】月【 15 】日

公共资源交易平台投标专用

鉴于：

甲方有信息化业务入驻【濮阳移动】政务云需求。乙方作为基础电信运营商且有丰富的集团客户通信服务经验和较强的服务能力，具备经营本合同相应业务的经营资质。依据《中华人民共和国合同法民法典》及其他有关法律、行政法规，遵循平等、自愿、公平和诚实信用的原则，双方就乙方向甲方有偿提供集团客户信息化服务事项协商一致，订立本合同。

第一条 合作内容

1.1 乙方在现有技术条件下、现有网络覆盖范围内，确保项目合法合规情况下，为甲方有偿提供云主机、云存储及相应的网络接入服务等。

（1）云主机：云主机是通过虚拟化技术整合计资源，提供按需使用的计算资源服务，可以根据需求选择不同规格的云主机服务。

（2）云存储：是指通过集群应用、网格技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统。

（3）网络接入：是指为客户的云主机提供网络接入服务。

1.2 乙方为甲方提供的具体服务相关具体要求详见【附件 1：云资源服务清单】。

第二条 资费标准和支付方式

2.1 甲方按照云资源实际使用情况，向乙方支付费用，本合同项下甲方应当向乙方支付的服务费用共计【13385326】元（大写：壹仟叁佰叁拾捌万伍仟叁佰贰拾陆），费用明细详见【附件 1：云资源服务清单】。

2.2 合同项下所有款项由甲方向乙方以如下方式及比例支付：

合同期【壹】年，业务合同期内甲方须于 2023 年 3 月 31 日前一次性向乙方支付的费用为：【13385326】元（大写：壹仟叁佰叁拾捌万伍仟叁佰贰拾陆 ）。

上述合同总价是含税价格，为固定不变价，如在使用过程中需对硬件资源进行调整，变更后以实际使用资源费用标准结算。

（1）费用结算：本合同中甲乙双方之间发生的所有费用均以人民币结算和支付。

（2）云服务业务在乙方将云主机、云存储等资源分配到位开始计费。

（3）乙方按照双方确认的账单金额开具发票，甲方应在收到发票后【15】日内支付相应费用。

2.3 甲方按照上述约定的结算周期将本合同项下的业务费用支付到以下银行账户：

乙方名称：【中国移动通信集团河南有限公司濮阳分公司】

纳税人识别号：【9141090071675895XC】

地址：【濮阳市卫河北路 36 号】

公共资源交易平台投标专用
AE2019E0776462E1462A8B6B2EA14DB9

户名：【中国移动通信集团河南有限公司濮阳分公司】

开户行：【中国工商银行濮阳分行华龙区支行】

账号：【1712020629201020591】

任何一方如需改变上述账户信息，应提前十（10）日以书面通知另一方。如一方未按本合同规定通知而使另一方遭受损失的，应予以赔偿。

2.4 结算周期内甲方向乙方支付的费用为：结算金额＝Σ（服务费±违约金）（说明：如甲方违约则使用“＋”，若乙方违约则使用“－”）。

2.5 结算方式采用【转账】的形式。

2.6 在甲方支付本合同项下的服务费之前，乙方应当向甲方开具相应金额的【普通】发票。甲方将本合同项下的业务费用支付到本合同所指定的银行账户即完成本合同的付款义务.

2.7 甲方如对乙方提供的产品和服务的费用产生异议，须于乙方向甲方通知相关费用之日起【15】日内向乙方提出，否则视为对费用的认可。

第三条 服务期限

本合同自双方签字盖章之日起生效，有效期【壹】年。

第四条 双方的权利与义务

4.1 甲方的权利和义务

4.1.1 甲方应严格遵守《中华人民共和国网络安全法》、《中华人民共和国电信条例》、《互联网信息服务管理办法》、《中华人民共和国反电信网络诈骗法》等有关法律法规规定，不得从事任何违法经营活动。

4.1.2 在本合同有效期内，甲方有权要求乙方根据本合同约定向甲方提供相应的服务。

4.1.3 甲方应本合同的约定，及时足额向乙方支付各项费用。

4.1.4 甲方同意乙方有权协同第三方从事部分合同约定的乙方服务工作。但是，乙方应对第三方的服务行为向甲方承担责任。

4.1.5 甲方在申请使用本合同业务时，必须向乙方提供真实、准确的注册信息，包括但不限于甲方的姓名/单位名称（及法定代表人/负责人姓名）、身份证件号码/统一社会信用代码、住址/住所、联系人、联系方式、邮政编码、电子邮件地址等，以及注册资料，包括但不限于身份证件/营业执照（及税务登记证）等有效证件的复印件（单位证件应加盖公章）。如注册信息和注册资料有任何变动，应当及时更新，甲方未及时、准确、完整更新有关信息并通知乙方的，由此带来的任何损失及法律责任全部由甲方自行承担。

4.1.6 如甲方拒绝向乙方提供真实、准确的注册信息和注册资料，或者冒用他人证件，或者使用伪造、变造的证件的，乙方依法有权拒绝为甲方提供或继续提供服务，由此带来的任何损失及法律责任全部由甲方自行承担。

4.1.7 甲方承诺：

公共资源交易平台投标专用
AE2014BC7646E1A8D48BC88A14DB9

4.1.7.1 甲方在使用业务用于非经营性或经营性互联网信息服务时，应建设并与工信部或省管局对接信安系统，保证该系统覆盖本协议分配的网络资源，甲方应向乙方出示信安系统评测结果通知单，并开展相关工作。如果甲方利用乙方提供的服务进行的活动需要获得国家有关部门的许可或批准的，应获得该有关的许可或批准。包括但不限于以下内容：如果甲方的网站提供非经营性互联网信息服务的，必须办理非经营性网站备案，并保证所提交的所有备案信息真实有效，在备案信息发生变化时及时在备案系统中提交更新信息；如甲方的网站提供经营性互联网信息服务的，甲方应自行向当地通信管理部门申请取得相应的增值电信业务经营许可证；如甲方经营互联网游戏网站的，甲方应依法获得网络文化经营许可证；如甲方经营互联网音、视频网站的，甲方应依法获得信息网络传播视听节目许可证；若甲方从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。

甲方理解并认可，以上列举并不能穷尽甲方进行经营或非经营活动需要获得国家有关部门的许可或批准的全部类型，甲方应获得有关的许可或批准并应在服务期内持续有效，同时还应符合国家及地方颁布相关法律法规之要求。

4.1.7.2 除乙方明示许可外，甲方不得修改、翻译、改编、出租、转许可、在信息网络上传播或转让乙方提供的软件及产品，也不得反向工程、反编译或试图以其他方式发现乙方提供的软件及产品的源代码。

4.1.7.3 若本合同业务涉及第三方软件之许可使用的，甲方同意遵守相关的许可协议的约束。

4.1.7.4 不利用乙方提供的资源和服务上传、下载、储存、发布如下信息或者内容，不为他人发布该等信息提供任何便利：

（1）反对宪法所确定的基本原则的；

（2）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（3）损害国家荣誉和利益的；

（4）煽动民族仇恨、民族歧视、破坏民族团结的；

（5）破坏国家宗教政策，宣扬邪教和封建迷信的；

（6）散布谣言，扰乱社会秩序，破坏社会稳定的；

（7）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（8）侮辱或者诽谤他人，侵害他人合法权利的；

（9）含有虚假、有害、胁迫、侵害他人隐私、骚扰、侵害、中伤、粗俗、猥亵、或其它道德上令人反感的内容；

（10）含有中国法律、法规、规章、条例以及任何具有法律效力之规范所限制或禁止的其它内容的。

4.1.7.5 不进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，

公共资源交易平台供标专用

网站或空间中含有或涉嫌散播：病毒、木马、恶意代码，及通过虚拟服务器对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP 欺骗、DOS 等）。

4.1.7.6 不运行影响乙方服务器正常工作的程序、进程，不进行任何改变或试图改变乙方提供的系统配置或破坏系统安全的行为。

4.1.7.7 不将本合同业务用于相关业务或产品故障可能会导致死亡、严重人身伤害，或严重的物理或环境损害（以下简称“高风险使用”）的任何应用或情况。高风险使用的情况包括但不限于：飞机或其他大型交通工具、核[illegible]或化工设施、生命支持系统、植入式医疗设备、机动车辆或武器系统；但是，高风险使用不包括，出于管理目的而利用产品来存储配置数据，利用工程和/或配置工具或利用其他非控制性应用程序，以及在上述使用情形中即使出现故障，也不会导致死亡、人身伤害或严重的物质或环境损害的任何应用或情况。这些非控制性应用程序可能会与控制性应用程序进行通信，但不得直接或间接地对控制功能负责。

4.1.7.8 不利用乙方提供的服务从事损害乙方合法权益及第三方合法权益的行为。

4.1.7.9 不从事其他违法、违规或违反本合同条款的行为。

4.1.7.10 如乙方发现甲方违反上述条款的约定，有权根据情况采取相应的处理措施，包括但不限于立即中止服务、终止服务或删除相应信息等。另外，如果第三方机构或个人对甲方提出质疑或投诉，乙方将通知甲方，甲方有责任在规定时间内进行说明并出具证明材料，如甲方未能提供相反证据或甲方逾期未能反馈的，乙方将采取包括但不限于立即中止服务、终止服务或删除相应信息等处理措施。因甲方未及时更新联系方式或联系方式不正确而致使未能联系到甲方的，亦视为甲方逾期未能反馈。甲方同意，乙方对因采取上述措施产生的后果不承担责任。

4.1.8 未经乙方书面同意，甲方不得将乙方的软件、技术、设施等用于双方合作项目以外的其他用途，且不得向第三方透漏、转让。若甲方违反本条款，乙方有权要求甲方赔偿损失，终止协议。

4.1.9 未经乙方书面同意，甲方不得擅自使用中国移动的企业及品牌名称和标识、乙方的地方性品牌的名称和标识。否则，乙方有权解除合同并要求甲方赔偿损失。

4.1.10 甲方承诺不利用乙方提供的本合同项下服务从事任何下列情形之一的行为：涉案涉诈、IP 违规翻墙、资质与互联网网络接入资源使用用途不一致、超范围经营、层层转租、发布不良信息、参与“挖矿”活动、黑名单网站接入、未备案接入等违法违规问题。发现甲方使用乙方提供的本合同项下服务存在涉嫌上述情况的，乙方有权根据情况采取相应的处理措施，包括但不限于立即中止服务、终止服务或删除相应信息等。

4.1.11 甲乙双方同意，上述 4.1.5-4.1.10 约定的情形从根本上违背本合同目的。乙方有权采取包括但不限于各种技术手段在内的措施检测识别、排查处置甲方使用乙方提供的本合同项下服务的行为，发现涉嫌上述情形的，乙方有权根据危害程度，决定单方解除本合同，由此产生的责任与后果由甲方承担。

4.1.12 甲方有责任对自身信息系统的安全状况负责，并定期对自身信息系统进行安全状况检

公共资源交易平台投标专用

查。甲方不应在本合同业务平台之上安装、使用盗版软件；甲方对自己行为（如自行安装的软件和进行的操作）所引起的结果承担全部责任。甲方应积极配合国家相关部门和乙方对网络安全事件的跟踪、调查，并提供相关的信息和资料。

4.1.13 甲方应向乙方提交执行本协议的联系人和管理用户网络及本合同业务平台上各类产品与服务的人员名单和联系方式并提供必要的协助，如以上人员发生变动，甲方应自行将变动后的信息进行在线更新并及时通知乙方。因甲方提供的人员的信息不真实、不准确、不完整，以及因以上人员的行为或不作为而产生的结果，均由甲方负责。

4.1.14 甲方了解乙方无法保证其所提供的服务毫无瑕疵，但乙方承诺不断提升服务质量及服务水平。所以甲方同意：即使乙方提供的服务存在瑕疵，但上述瑕疵是当前行业技术水平所无法避免的，其将不被视为乙方违约。甲方同意和乙方一同合作解决上述瑕疵问题。6.1.3 甲方应当根据其所使用的业务的要求向乙方提供真实有效的证件、资料和信息（包括但不限于甲方单位及相关授权人真实有效的营业执照、身份证、授权委托书等证件，以及白名单的相关资料等）。

4.1.15 甲方承诺并保证不利用乙方提供的服务进行任何违反国家政策、法律法规以及侵犯乙方或第三方合法权益的行为。甲方不得利用互联网从事危害国家安全，泄露国家机密等犯罪活动；不得制作、复制和传播有碍社会治安和有伤风化的信息。否则，乙方有权立即停止向甲方提供所有产品和服务并解除本合同，一切后果由甲方承担。

4.1.16 甲方应本合同的约定，及时足额向乙方支付各项费用。如甲方未能按照约定及时向乙方支付云服务费用，乙方将采取包括但不限于立即中止服务、终止服务或删除相应信息等处理措施。乙方对因采取上述措施产生的后果不承担责任。

4.1.17 甲方如对乙方提供的产品和服务的费用产生异议，须于乙方向甲方通知相关费用之日起【15】日内向乙方提出，否则视为对费用的认可。

4.1.18 甲方应授权一名员工作为联系人，负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。甲方联系人需提供乙方所需的身份确认资料。甲方联系人如发生变更，需以书面形式通知乙方。

4.1.19 甲方开通使用乙方提供的相关产品时，需遵守对应的产品使用说明。甲方未按约定和相关要求使用产品的，相关责任由甲方承担。

4.1.20 甲方成为乙方集团客户后，如果乙方提供了服务账号，甲方应妥善保管乙方提供的服务账号和甲方设定的服务密码。服务账号和密码是甲方办理相关业务的凭证，凡使用服务密码进行的任何操作行为均被视为甲方或甲方授权行为。如因甲方服务账号和密码保管不善等原因发生服务中断、业务变更、高额费用等情况，甲方应立即以书面形式通知乙方，乙方应采取可行的补救措施。甲方应当承担因账号和密码保管不善产生的费用。

4.1.21 如因甲方提供的相关资料不准确、不真实、不完整或变更后未通知乙方等原因，使乙方无法将服务提供给甲方，甲方承担由此造成的责任和后果。

公共资源交易平台投标专用
AE2A190C7646D1162A8BC8814DB9

4.1.22 在乙方云资源发放到位 4 后，甲方负责自身应用系统的维护工作，本合同另有约定的除外。

4.1.23 未经乙方同意，甲方不得将乙方的软件、技术、设施等用于双方合作项目以外的其他用途，且不得向第三方透漏、转让，若甲方违反本条款，乙方有权要求甲方赔偿损失，终止协议。

4.1.24 未经乙方书面同意，甲方不得擅自使用中国移动的企业及品牌名称和标识、乙方的地方性品牌的名称和标识。否则，乙方有权解除合同并要求甲方赔偿损失。

4.1.25 甲方负责虚拟机上操作系统、应用软件以及病毒的防护，定期修补系统漏洞和病毒库升级。甲方在虚拟机上所需要安装的软件版权/许可/使用权由甲方自行解决，如果由此产生法律纠纷，与乙方没有任何关系，乙方也不应对此或对第三方承担任何责任或者义务。

4.1.26 甲方投资的相关设备设施及软件产权归属甲方，乙方投资的相关设备设施及软件产权归属乙方。

4.2 乙方的权利和义务

4.2.1 乙方负责保证网络畅通，提供 24 小时不间断电源和标准机房环境，为保证系统正常运行所需的预防性维护、日常维护支持、网络调整支持、数据备份支持等。如果出现紧急技术问题，在甲方通过电话或传真通知乙方的情况下，乙方的工程师应在【8】小时内予以答复。如果甲方要求紧急处理，乙方应在收到甲方通知后的【4】小时内赶到机房现场。当合同系统提供的业务中断时，乙方在提供远端服务的同时，须在收到甲方通知后【24】小时内赶到机房现场，因不可抗力致使乙方未按时到达现场的除外。

4.2.2 乙方派专人负责虚拟机服务器的日常维护和监控，定期对云主机进行系统漏洞扫描，并将风险情况告知甲方进行整改。在乙方从事云服务过程中，乙方人员携带相关证件及单位证明，与甲方相关部门联系并办理相关手续，甲方应及时提供相关配合。

4.2.3 乙方具有保证云平台数据安全的义务，不得泄露客户数据，不得擅自留存、使用、泄露或者向他人提供政务数据。发现数据安全隐患应及时排除，未经许可，乙方不得对存放在虚拟机上的数据进行修改。

4.2.4 乙方应妥善进行个人信息保护，如甲方需要与乙方签订个人信息保护合同，乙方应积极配合，并按照合同约定处理个人信息，不得超出约定的处理目的、处理方式等；委托合同不生效、无效、被撤销或者终止的，将个人信息返还个人信息处理者或者予以删除，不得保留。未经甲方同意，不得转委托他人处理个人信息。

4.2.5 乙方从事云平台服务等工作，需遵守甲方的网络安全政策规定、信息安全等级保护要求、技术标准，落实安全管理和防护措施，接受甲方相关部门的网络安全监管。

4.2.6 乙方进行检修线路、设备搬迁、工程割接、网络及软件升级或其他网络设备进行调试、维护工作，或因其他可预见性的原因可能影响甲方使用本合同约定服务的，应提前通知甲方，甲方应给予必要的配合。

公共资源交易平台招标专用

4.2.7 乙方受理甲方的故障申报，应及时安排故障处理。乙方按维护及业务规程的有关规定，为甲方提供优质服务。

4.2.8 在合同有效期内，乙方有责任按照国家标准负责系统的日常运行维护工作。保障系统的正常运行，如发生故障，及时响应。

4.2.9 如果有甲方投资的相关设备设施及软件，因甲方设备问题导致乙方无法正常提供本合同约定服务的，由甲方承担相应责任。

4.2.10 因第三方实施破坏、网络攻击非乙方原因导致甲方不能正常使用乙方产品和服务的，不视为乙方违约，乙方不承担相应责任。

4.2.11 乙方有权根据本合同约定要求甲方及时足额支付各项费用。

4.2.12 乙方应对其所委托的代为向甲方提供本合同项下服务的第三方的服务行为向甲方承担责任，包括保证其提供的服务质量符合本合同约定，并对其服务瑕疵向甲方承担违约责任。

4.2.13 因甲方员工与乙方存在电信服务合同关系，若在本合同履行过程中，甲方员工就与本合同有关的服务提出异议时，为保证甲方员工利益，乙方有权对提出异议的甲方员工暂停提供与本合同有关的甲方员工个人服务，并由三方进行协商。待三方意见一致时，再向提出异议的甲方员工恢复本合同服务，乙方无需因此向甲方承担违约责任。甲方员工如对已经提供的服务要求乙方承担责任时，该责任由甲方向乙方承担。

4.2.14 当本合同到期终止前至少【10】个工作日，乙方以【书面】形式告知甲方合同即将结束，甲方应于收到通知之日起【3】个工作日内【书面】通知乙方是否续签。如果合同续签，甲方应于收到通知之日起在【10】个工作日内完成与乙方的续签工作，如合同终止但续签尚未完成，期间产生的云资源费用由甲方承担。如果合同不再续签，甲方应于收到通知之日起【15】个工作日内，完成业务数据迁移删除。若甲方收到通知后不配合，乙方将自向甲方发出通知之日起默认继续保存业务数据【30】个自然日，逾期将不再保留甲方的数据，甲方应在上述期限届满前自行做好数据备份工作，因未及时备份数据所产生的一切后果由甲方自行承担后删除业务数据，由此产生一切后果由甲方负责。

4.2.15 基于电信技术的发展，按照相关法律法规、政府指令、行业规划或业务调整的需要，乙方可以停止提供本协议项下的服务（包括但不限于网络服务、用户服务、电信服务及其他相关服务），但应提前向甲方发送通知。如遇紧急突发情况，乙方可以立即停止提供本协议项下的服务，但应尽量提前向甲方发送通知。甲方同意，乙方对因采取上述措施产生的后果不承担责任。

第五条 用户信息和数据

5.1 为了保障甲方使用本协议项下服务的安全以及不断改进本合同业务质量，本合同业务系统将记录并保存甲方登录和使用本协议项下服务的相关信息。

5.2 甲方的用户信息和数据将在下述情况下部分或全部被披露：

5.2.1 经甲方同意，向第三方披露；

公共资源交易平台技术专用

5.2.2 根据法律法规的有关规定，或者行政、司法机关的要求，向第三方或者行政、司法机关披露；

5.2.3 如果甲方出现违反中国有关法律法规的情况，需要向第三方披露；

5.2.4 为提供甲方所要求的软件或服务，而必须和第三方分享甲方的用户信息和数据。

5.3 乙方仅得按当前行业技术水平提供相应的安全措施以使本合同业务系统存储的用户信息和数据不丢失，不被滥用和篡改，这些安全措施包括向其他服务器备份数据和对用户密码加密。鉴于计算机及互联网的特殊性以及网络安全技术的局限性，甲方理解，尽管有这些安全措施，但本合同业务系统仍然不能保证甲方的用户信息和数据的绝对安全。

5.4 对于甲方通过本合同业务平台上传、下载、储存、发布的内容，乙方有权根据国家相关法律法规和网络信息安全管理部门的规定，以及本协议其他约定，进行必要的监督和审查。

5.5 甲方理解并同意：在向甲方提供服务的过程中，基于运维管理等需要，乙方有可能对甲方在合同业务系统中存储的数据进行迁移、维护等操作，上述数据迁移、维护操作是乙方为向用户提供本合同业务所必须的，不构成对甲方的隐私资料、保密信息的任何侵犯。甲方同意并授权乙方（在履行保密义务并采取适当保护措施的情况下）可以进行上述数据迁移、维护操作。甲方保证其上述授权行为已经获得了所有必要的同意、许可并遵从了所有可适用的法律法规的要求。

5.6 除法定及甲乙双方另行约定外，自本协议约定的服务期满或因任何原因导致本协议提前终止的，乙方将自终止之日起继续存储甲方的数据【1】日，逾期将不再保留甲方的数据，甲方应在上述期限届满前自行做好数据备份工作，因未及时备份数据所产生的一切后果由甲方自行承担。

第六条 知识产权

6.1 甲方应保证提交给乙方的素材、对乙方服务的使用及使用本合同业务所产生的成果未侵犯任何第三方的合法权益。如有第三方基于侵犯版权、侵犯第三人之权益或违反中国法律法规或其他适用的法律等原因而向乙方提起索赔、诉讼或可能向其提起诉讼，则甲方应赔偿乙方因此承担的费用或损失，并使乙方完全免责。

6.2 如果第三方机构或个人对甲方使用本合同业务所涉及的相关素材的知识产权归属提出质疑或投诉，甲方有责任出具相关知识产权证明材料，并配合乙方相关投诉处理工作。

6.3 甲方承认乙方向甲方提供的任何资料、技术或技术支持、软件、服务等的知识产权均属于乙方或第三方所有。除乙方或第三方明示同意外，甲方无权复制、传播、转让、许可或提供他人使用上述资源，否则应承担相应的法律责任。

第七条 保密条款

7.1 “保密信息”是指本协议拥有信息的一方（“提供方”）根据本协议向另一方（“接受方”）提供的信息，或接受方在本协议履行过程中从提供方处获知的信息。保密信息包括但不限于的：技术信息、商业信息、商业秘密、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法和其他保密信息，本协议的条款和与本协议有关的其他信息，本协议履

公共资源交易平台电子签章专用

行过程中形成的所有信息、数据、资料、意见、建议等。

7.2 保密信息只能由接受方及其人员为本协议目的而使用。除非本协议另有约定，对于提供方提供的任何保密信息，未经提供方事先书面同意，接受方及其知悉保密信息的有关人员均不得直接或间接地以任何方式提供或披露给任何第三方。甲方理解并同意，乙方及其关联公司可通过业务受理系统登记、纸质档案，通过网络接收、读取并记录等方式，以提供电信服务为目的，在业务活动中收集、使用甲方提供的和甲方使用服务过程中形成的信息。乙方有权依法对包含甲方在内的整体用户数据进行分析并加以利用，未经甲方同意，乙方不向除乙方关联公司外的第三方提供甲方信息。乙方关联公司，是指中国移动通信集团公司及其在中华人民共和国境内直接或间接控股的主营通信业务的公司，以及上述公司的合法继承公司。

7.3 双方不得向任何人透露用户的信息、资料以及交易记录，除国家法律、行政法规另有规定外，双方均有权拒绝除用户本人以外的任何单位或个人的查询；同时，双方应尽合理努力将电子支付交易数据以安全方式保存，并防止其在公共、私人或内部网络上传输时被擅自查看或非法截取。

7.4 接受方的律师、会计师、承包商和顾问为提供专业协助而需要了解保密信息时，接受方可向其披露保密信息，但是，其应要求上述人员签订保密协议或按照有关职业道德标准履行保密义务。接受方应向提供方承担因己方聘请的上述专业顾问违反保密约定而给提供方造成的任何损失。

7.5 如相关政府部门或监管机构要求接受方披露任何保密信息，接受方可在该政府部门或机构要求的范围内做出披露而无需承担本协议项下的保密责任。但前提是，该接受方应立即将需披露的信息书面通知提供方，以便提供方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且接受方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。保密信息不包括以下任何信息：（1）非因违反本协议所致，已进入公众领域的信息；（2）在提供方依据本协议做出披露前，接受方已合法拥有的信息；（3）接受方从有权披露的第三方获得的信息；及（4）接受方独立开发的信息，未使用任何保密信息。

7.6 双方应严格遵守保密条款之约定，严格履行保密义务，直至有关保密信息合法公开之时止。本协议或其任何条款的终止、中止、失效、无效均不影响本保密条款的有效性及对甲乙双方的约束力。

7.7 由于保密信息接受方未履行保密义务给提供方造成损失的，接受方应当赔偿由此给提供方造成的损失。

7.8 在任何情形下，本合同约定的保密义务应永久持续有效。

第八条　违约责任

8.1 任何一方不履行本合同约定的义务或履行义务不符合本合同约定的，均构成违约，应承担违约责任。

8.2 甲方未按照本合同约定支付合同款项的，从逾期的次日起计算违约金，每滞后 1 天收取未缴金额的【1‰】。违约金总额超过所欠金额的【6%】时，乙方有权解除本合同，并保留进一步追偿

公共资源交易平台专用

的权利。

8.3 如甲方未按本合同约定或国家法律法规规定及时办理相关备案或审批手续，因此产生的一切责任和后果均由甲方承担。根据国家法律法规、通信管理部门的规定或通知，乙方有权中断、终止为甲方提供本协议项下的全部或部分业务，且无需承担任何违约责任。

8.4 乙方在履行本合同时，不得对甲方的通信网络、信息网络发起任何形式的攻击、预留软件后门、或内置黑客软件等，且乙方应当加强对其工作人员的工号、权限管理和教育，以避免前述攻击的发生。在发现乙方或乙方人员对甲方或甲方网管网络实施前述攻击时，甲方将立即解除本合同，终止和乙方的任何合作。

8.5 乙方在进行网络调整和维护时需要短时间中断服务，或者由于 Internet 上骨干网通路的阻塞造成甲方服务器访问速度下降，双方认同属于正常情况，不视为乙方违约。

8.6 下列情况下乙方有权单方终止本合同，并停止向甲方提供服务。由此给甲方造成的损失，乙方不承担责任，并有权要求甲方承担违约和赔偿责任：

（1）甲方（包括联系人）提供虚假证照的；

（2）甲方利用乙方提供的产品和服务实施违反国家法律、法规和政策的活动；

（3）甲方利用乙方提供的产品和服务从事其他不当用途或侵犯第三方的合法权利；

（4）乙方根据国家有关部门的要求停止为甲方提供相关服务。

8.7 乙方仅对因其过错给甲方造成的直接损害结果承担赔偿责任，且不包括第三方提出的索赔要求、数据丢失或损坏的损失，不包括经营损失等一切间接损失。无论何种情况，乙方对本协议项下的违约赔偿总额不超过本协议项下已支付的服务费用的总和。

第九条　不可抗力及免责条款

9.1 本合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况。

9.2 由于不可抗力事件，致使一方在履行其在本合同项下的义务过程中遇到障碍或延误，不能按约定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（“受阻方”），只要满足下列所有条件，不应视为违反本合同：（1）受阻方不能全部或部分履行其义务，是由于不可抗力事件直接造成的，且在不可抗力发生前受阻方不存在迟延履行相关义务的情形；（2）受阻方已尽最大努力履行其义务并减少由于不可抗力事件给另一方造成的损失；（3）不可抗力事件发生时，受阻方立即通知了对方，并在不可抗力事件发生后的十五(15)天内提供有关该事件的公证文书和书面说明，书面说明中应包括对延迟履行或部分履行本合同的原因说明。

9.3 不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方应可延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

9.4 如果不可抗力事件的影响持续达三十（30）日或以上时，双方应根据该事件对本合同履行的影响程度协商对本合同的修改或终止。如在一方发出协商书面通知之日起十（10）日内双方无法就此达成一致，任何一方均有权解除本合同而无需承担违约责任。

公共资源交易平台专用

9.5 乙方对下述事项不承担责任：（1）第三方对甲方提出的索赔要求；（2）甲方的记录或数据的丢失或损坏；（3）甲方的经营损失等一切间接损失。

9.6 如因乙方难以避免、难以排除的技术或网络故障或第三方原因造成甲方无法使用本协议项下服务的，不视为乙方违约，但乙方应尽合理努力争取在最短时间内解决，对此双方无异议。鉴于计算机、移动通信网络及互联网的特殊性，因黑客、病毒、电信部门技术调整和骨干线路中断等引起的事件，在乙方能够出具相关合理证明材料的情况下，甲方亦认同不属于乙方违约。

第十条　争议解决

10.1 本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决均应适用中华人民共和国法律。

10.2 如果任何争议或权利要求起因于本合同或与本合同有关或与本合同的解释、违约、终止或效力有关，都应由双方通过友好协商解决。协商应在一方向另一方送达关于协商的书面要求后立即开始。

10.3 如果在一方提出协商要求后的十(10)天内，双方通过协商不能解决争议，则双方同意向乙方住所地人民法院提起诉讼。

10.4 诉讼进行过程中，除双方有争议的部分外，本合同其他部分仍然有效，双方应继续履行。本合同全部或部分无效的，争议解决条款依然有效。

第十一条　其他约定

11.1 本合同一式【肆】份，双方各持【贰】份，具有同等法律效力。

11.2 对于合同未尽事宜、双方可签订补充合同对本合同中的问题做出补充、说明、解释。本合同的补充合同作为本合同不可分割的一部分，与本合同具有同等的法律效力。

11.3 本协议附件作为本协议的一部分，与本协议具有同等法律效力。

11.4 在本协议有效期内，双方可以通过友好协商，对本协议相应条款进行变更或者解除本协议。任何一方欲变更或解除本协议，应提前 30 日向另一方提交书面说明。单方面解除协议的一方，应对另一方因此遭受的损失承担全部赔偿责任。

第十二条　本合同附件

附件 1：云资源服务清单

（以下无正文）

公共资源交易平台投标专用
AE2C19CEC7764E1A9246B588EA14DB9

八、投标人中小企业、监狱企业或残疾人福利性单位声明函（如果有的话）

我公司非中小企业、监狱企业或残疾人福利性单位

中小企业声明函（工程、服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司

（联合体）参加（单位名称）的（项目名称）采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合 体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

（标的名称），属于（采购文件中明确的所属行业）；

承建（承接）企业为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

（标的名称），属于（采购文件中明确的所属行业）；承建（承接）企业为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

公共资源交易平台 技标专用
AB2C19CEC7764621A628BC88EA4DB9

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：　　日期：

监狱企业声明函

本企业郑重声明，根据《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68 号），本企业_____（是、不是）监狱企业。后附省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业证明文件。

本企业对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日　期：

残疾人福利性单位声明函

本企业郑重声明，根据《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库[2017]141 号），本企业_____（是、不是）残疾人福利性单位。

本企业对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日　期：

注：如果投标人是中小企业或残疾人福利性单位的，提供《声明函》即可，若中标，《声明函》将随中标结果公开，接受社会监督；如果是监狱企业，还需提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

公共资源交易平台投标专用
AE2C15CEC17646E1AC9A82C88EA14DB9

九、招标文件要求的其它材料及投标人认为有必要提供的材料

9.1 投标人 IDC 机房达到 A 级标准的证明材料



证书编号：CNCA2023-DJRZGA-2023021

数据中心基础设施等级认证

CQC

【经审核】

河南移动南阳分公司IDC数据中心

注册地址：南阳市宛城区张衡路1266号

项目地址：南阳市宛城区张衡路1266号

符合数据中心基础设施等级认证国标A级

[认证依据] T/CCUA 001-2023 数据中心基础设施等级评价；
GB 50174-2017 数据中心设计规范。

[认证范围] 河南移动南阳分公司IDC数据中心基础设施，认证覆盖内容见附录（附录共1页）。

签发人：

发证日期：2023年08月23日

证书有效期：2023年08月23日 - 2026年08月22日

北京国信天元质量测评认证有限公司



公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

9.2 投标人 IDC 机房或本地通信机房具有 2 路 10KV 高压电力专线从不同变压器接入的证明材料

9.2.1 投标人机房 A 级证书附录页电气部分


证书编号：CNCA2[illegible]DJRZGA2023021

数据中心基础设施等级认证

GQC

【经审核】

河南移动南阳分公司IDC数据中心

注册地址：南阳市宛城区张衡路1266号

项目地址：南阳市宛城区张衡路1266号

符合数据中心基础设施等级认证国标A级

[认证依据] T/CCUA 001-2023 数据中心基础设施等级评价；
GB 50174-2017 数据中心设计规范。

[认证范围] 河南移动南阳分公司IDC数据中心基础设施，认证覆盖内容见附录（附录共1页）。

签发人：

[illegible]期：2023年08月23日

证书有效期：2023年08月23日 - 2026年08月22日

北京国信天元质量测评认证有限公司

证书附录页

【证书编号】 CNCA20[illegible]-DJRZGA-2023021[illegible]

【获证数据中心名称】 河南移动南阳分公司IDC数据中心

【认证范围】

中国移动通信集团河南有限公司南阳分公司IDC数据中心位于南阳市宛城区张衡路1266号，本次服务对数据中心机柜编号：R02列至R07列、A列至K列总共248个机柜进行国标等级认证技术服务。

【项目详细认证内容】

电气系统：

机房供配电系统采用"双路市电＋后备柴油发电机"的供电方式，机房分别从两路不同的变电站引入两路10kV市电专线分别至一层配电室，经过一层配电室内的变压器降压后为数据中心IT设备与动力设备供电。正常情况，两路市电同时为机房IT设备与动力设备供电；当一路电源失电时，另一路市电通过高压母联开关为失电线路提供电源；且低压配电系统设置了母联备自投装置，当一路低压电源失电后，可由另一路低压电源通过母联开关为失电电源供电。当两路市电均失电时，通过低压柴油发电机分别为两段低压配电系统供电的方式为机房提供应急电源。机房在大楼柴油发电机室配置2台品牌为康明斯，型号为P1734C1，额定功率为1800kW的低压柴油发电机组，分别为机房提供应急备用电源。南侧机房配置4台品牌为艾默生，型号为Liebert eXM 200kVA系列的200kVA UPS，采用2N的运行方式，为南侧机房IT设备提供A\B两路电源。南侧机房每台UPS配置2组（40节/组）共80节品牌为南都，型号为6-GFM-200M的12V蓄电池。每台UPS电池后备时间满足机房使用需求。北侧机房配置4台品牌为艾默生，型号为Liebert NX 0300Ktk16FN01000系列的300kVA UPS，采用2N的运行方式，为北侧机房IT设备提供A\B两路电源。北侧机房每台UPS配置1组共240节品牌为南都，型号为GFM-660HR的2V蓄电池。每台UPS电池后备时间满足机房使用需求。

防雷接地系统：

机房采用联合接地方式，配变电所内高压系统的保护和工作接地以及低压系统的保护与工作接地、设备防静电接地、信息系统接地等与本建筑设备的保护接地及工作接地采用共用接地装置，并作等电位联结，大楼为机房提供专用的接地点；机房内设接地汇集排，机房内所有设备的金属外壳、各类金属管道、金属线槽、支架及金属构件等就近与接地汇集排相连接。

暖通系统：

南侧机房内配置5台品牌为艾默生，型号为P2100DA13FHM12E1D000P1000，制冷量为100kW的风冷型精密空调，及一台品牌为阿尔西，型号为OPTIMA.U.DXA90E2A5，制冷量为90.8kW的风冷型精密空调，采用运行方式为N+1，送风方式为地板下送风上回风。北侧机房内配置3台品牌为艾默生，型号为P2100-DA13FHM12E1D000P1000，制冷量为100kW的风冷型精密空调，及5台品牌为阿尔西，型号为OPTI-MA.U.DXA90E2A5，制冷量为90.8kW的风冷型精密空调，采用运行方式为N+1，送风方式为地板下送风上回风。

监控系统：

机房通过采集设备对机房环境参数和动力设备参数进行集中监控，监控对象包括：电量仪、UPS、精密空调、温湿度、漏水等。机房采用点式漏水检测设备，通过与监控管理计算机之间通讯，从而实现监控平台对漏水报警的实时监控。机房区域采用高清摄像机，分布在机房出入口及各个通道，机房无盲区，录像数据存储周期大于半年。机房在进口处设置(刷卡+指纹+刷脸)门禁一体机，进门刷卡、刷脸或指纹，机房在出口处设置出门按钮，出门按出门按钮。门禁系统可以记录进出机房的时间及使用者身份。

装饰装修系统：

机房无吊顶，顶面喷涂白色乳胶漆饰面。

机房墙面采用乳胶漆饰面。

机房采用600mm×600mm的防静电地板，地面做石板地面。

综合布线系统：

机房综合布线系统通过弱电桥架采用上走线的安装方式连接至各机柜，并与建筑装饰、电气、空调、消防等协调一致，顶部距离房顶及其他障碍物满足使用需求。

北京国信天元质量测评认证有限公司
地址：北京市大兴区欣雅街15号院5号楼4层413
中国国家认证认可监督管理委员会：http://www.cnca.gov.cn/
中国计算机用户协会数据中心分会：https://cra-ccua.org.cn/

9.2.2 投标人与南阳供电公司签订两路电力的调度协议

南阳供电公司调度控制中心

调度协议

中国移动通信集团河南有限公司南阳分公司

二零一四年九月

486766

公共资源交易平台投标专用
AE2C19CEC77646E1A62A8BC88EA14DB9

调 度 协 议

本并网调度协议(以下简称本协议)由下列双方签署:

甲方： 南阳供电公司调度控制中心

法定住所：南阳市人民北路 268 号

乙方： 中国移动通信集团河南有限公司南阳分公司

法定住所：南阳市两相西路 666 号

为保证电力系统安全、优质、经济运行，规范调度和并网运行行为，维护协议双方的合法权益，根据《中华人民共和国电力法》、《中华人民共和国合同法》、《电网调度管理条例》以及国家其他有关法律、法规，本着平等、自愿、诚实信用的原则，双方经协商一致，签订协议如下:

1. 总则

1. 1 乙方用电设备接入甲方电网运行后， 应接受甲方电力调控中心统一调度管理。

1. 2 甲、乙双方应认真执行《电力法》《电网调度管理条例》及《南阳电力调度规程》 确保南阳电网安全、可靠、优质、经济运行，维护双方的合法权益。

1.3 乙方变电站值班人员必须熟知本地区电力系统调度管理的有

公共资源公易平台投标专用
AE2C15CEC77646E1A62F8BC88EA14DB9

关规定和业务术语，并经南阳供电公司调度控制中心配网调控班培训考试合格后，方可上岗。

1.4 若甲方或乙方的值班人员或通信方式发生变化，应及时通知对方，确保人员名单准确及通信畅通。

1.5 甲方供电线路名称发生变化时，由甲方负责及时通知乙方。

1.6 属配调调度管辖范围内设备一切操作，乙方值班人员必须得到甲方当值调度员正式命令后才能进行。

2. 接入电网条件

2.1 乙方接入南阳电网前必须具有接受电网统一调度的技术装备和管理设施，具体如下:

2.1.1 新投产设备已通过试运行和启动验收（必须有甲方电网管理部门的代表参加）；

2.1.2 接受电网统一调度的技术装备和管理设施齐备;

2.1.3 已向甲方电网管理部门提交齐全的技术资料;

2.1.4 与甲方调度的通信通道符合规定，并已具备投运条件;

2.1.5 按电力行业标准、规程设计安装的继电保护、安全自动装置已具备投运条件，电网运行所需的安全措施已落实;

2.1.6 有关的计量（考核）装置安装齐备并经验收合格;

2.1.7 具备正常生产运行的其他条件。

3. 调度关系:

3.1 甲方值班调度员与乙方值班员建立调度关系，乙方值班员在调度(许可)范围内必须接受甲方值班调度员的调度指令，以《南

公共资源交易平台投标专用
AE2C19CEC7C6A6E1A624BBC88EA14DB9

阳电力调度规程》作为调度管理的依据，当乙方现场规程与《南阳电力调度规程》有分歧时，以《南阳电力系统调度规程》为准。

3.2 乙方应组织值班员学习《电网调度管理条例》《南阳电力调度规程》及本协议，并经甲方调度部门考试合格持证后，才能接受调度指令。

3.3 甲方值班调度员有权发布调度管辖范围内所有设备的操作指令，并对下达指令的正确性负责；甲方调度许可的设备状态的改变需得到甲方值班调度员的许可后才能进行；乙方值班员应及时执行甲方值班调度员发布的调度指令，并对操作的正确性负责。

3.4 乙方检修线路时，操作前必须与甲方调度员联系，在做好相应安全措施后，由甲方下令操作。

3.5 乙方值班员应如实汇报现场运行情况，正确回答甲方值班调度员的询问，不得隐瞒事实。对于隐瞒事实、无正当理由拒绝执行调度指令、违反调度纪律或其他有关规程的，乙方值班员除按有关规定处理外，将取消值班员资格。

3.6 凡属甲方调度（许可）的设备，乙方不得自行操作，在遇有危及人身及设备安全的情况下乙方值班员可以按有关规程规定处理，并及时汇报甲方值班调度员。

4.运行方式及调度范围：

4.1 中国移动通信集团河南有限公司南阳分公司的供电线路为10KV钧移线、10KV康移线。

公共资源公共平台技术专用
AE2C19CFC7764CF1A62A8BC88EA14DB9

4.2 甲方调度范围：钓移 1 开关、康移 1 开关调度权属南阳调控中心。

4.3 乙方调度范围：钓移线、康移线、中国移动通信集团河南有限公司南阳分公司内其它设备属中国移动通信南阳分公司。

4.4 正常运行方式：钓移线运行带中国移动通信集团河南有限公司南阳分公司负荷，康移线为备用线路。

4.5 钓移线、康移线维护权归中国移动通信集团河南有限公司南阳分公司。

4.6 中国移动通信集团河南有限公司南阳分公司开闭所内有该公司进线钓移线、康移线之间的联络开关移 100，该开关断、合操作前；钓移线、康移线改变运行方式前，需报南阳配调值班人员，并得到许可后，方可进行操作，如未履行上述汇报、许可手续而擅自操作，造成的一切不良后果，均由中国移动南阳分公司单方承担。

5、检修及停送电管理

5.1 甲方计划检修工作需线路停电时，南阳调控中心运行方式专责应提前一周通知乙方，因临时检修需乙方线路停电时，应提前 24 小时通知乙方。

5.2 乙方因工作需要需甲方配合时，应于计划停电前一天 11:00 以前，由乙方停送电工作联系人，报南阳供电公司调控中心运行方式专责同意（事故处理除外），操作前后均由南阳配调与乙方联系，线路的停送电工作均按《电力安全工作规程》、《南阳

公共资源交易平台技术专用

11.5 当国家和政府制定的法律、法规、规定有变化时，调度（许可）范围变更时，应及时补充或修改本协议。

附件 1: 双方电话号码和联系人员名单

注：本协议（包括特别条款）的附件是本协议不可缺少的组成部分，与本协议具有同等法律效力。

南阳供电公司电力调度控制中心　　中国移动通信集团河南有限公司南阳分公司

（盖章）　　（盖章）

2014 年 9 月　　2014 年 9 月

公共资源交易平台投标专用
AE2[illegible]C77646E1A62A8BC88EA14DB9

附件 1：工作联系人员名单

南阳供电公司电力调度控制中心

电力调控中心主任：华大鹏　63805273　手机 13903778326

主管副主任：魏秋辉　63805256　手机 13903771956

自动化副主任：刘晓东　63805299　手机 13707639816

运行方式专责：

吉克威　63805261　手机 13838967695

孙小东　63805660　手机 13525122948

汤　浩　63805259　手机 13803778160

传　真：63805660

配网调控班：

班　　长：郑　凌　**63806273** 手机 13782173668

调 度 员：高丽霞 刘霞 惠运然 高娟 李新哲 吕巧玲 陈红 余江峰 杨庆卫 刘方 李新 贾学东 李长健 卞傲征

联 系 电 话：63231676　63807053　63806100

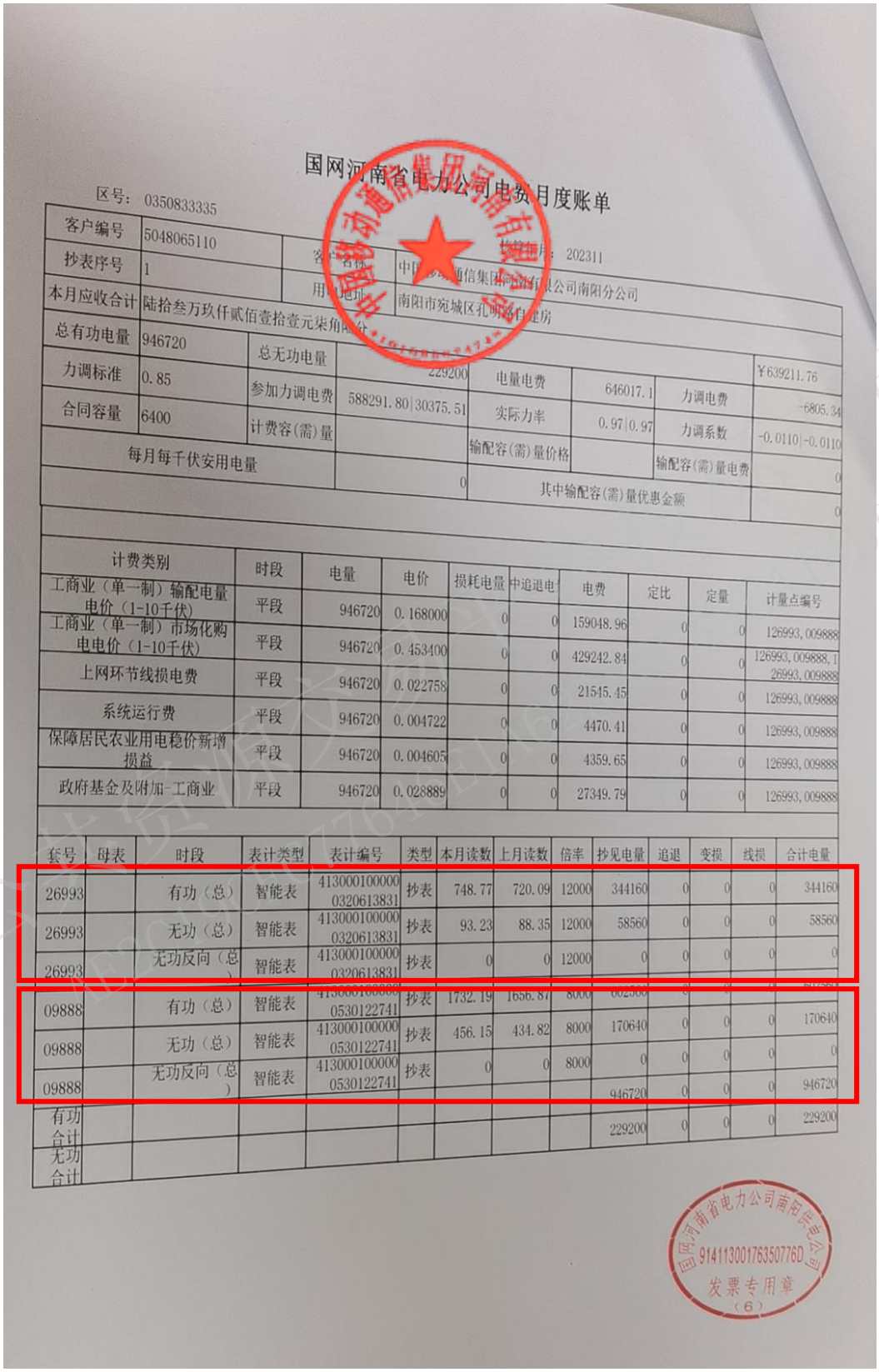
中国移动通信集团河南有限公司南阳分公司

主管领导：赵黎君 13837716990

停送电联系：陈旗　13837778663

公共资源交易平台投标专用
AE2C19CEC7646E1A62A8BC88EA14DB9

9.2.3 投标人 2 路电力月度缴费账单



国网河南省电力公司电费月度账单

区号：0350833335

客户编号	5048065110	客户名称	中国[illegible]通信集团河南有限公司南阳分公司			结算年月	202311
抄表序号	1	用电地址	南阳市宛城区孔明路自建房				
本月应收合计	陆拾叁万玖仟贰佰壹拾壹元柒角叁分						¥639211.76
总有功电量	946720	总无功电量	229200	电量电费	646017.1	力调电费	-6805.34
力调标准	0.85	参加力调电费	588291.80|30375.51	实际力率	0.97|0.97	力调系数	-0.0110|-0.0110
合同容量	6400	计费容(需)量		输配容(需)量价格		输配容(需)量电费	0
每月每千伏安用电量		0		其中输配容(需)量优惠金额			0

计费类别	时段	电量	电价	损耗电量	中追退电	电费	定比	定量	计量点编号
工商业（单一制）输配电量电价（1-10千伏）	平段	946720	0.168000	0	0	159048.96	0	0	126993,009888
工商业（单一制）市场化购电电价（1-10千伏）	平段	946720	0.453400	0	0	429242.84	0	0	126993,009888,126993,009888
上网环节线损电费	平段	946720	0.022758	0	0	21545.45	0	0	126993,009888
系统运行费	平段	946720	0.004722	0	0	4470.41	0	0	126993,009888
保障居民农业用电稳价新增损益	平段	946720	0.004605	0	0	4359.65	0	0	126993,009888
政府基金及附加-工商业	平段	946720	0.028889	0	0	27349.79	0	0	126993,009888

套号	母表	时段	表计类型	表计编号	类型	本月读数	上月读数	倍率	抄见电量	追退	变损	线损	合计电量
26993		有功（总）	智能表	413000100000 0320613831	抄表	748.77	720.09	12000	344160	0	0	0	344160
26993		无功（总）	智能表	413000100000 0320613831	抄表	93.23	88.35	12000	58560	0	0	0	58560
26993		无功反向（总）	智能表	413000100000 0320613831	抄表	0	0	12000	0	0	0	0	0
09888		有功（总）	智能表	413000100000 0530122741	抄表	1732.19	1656.87	8000	602560	0	0	0	170640
09888		无功（总）	智能表	413000100000 0530122741	抄表	456.15	434.82	8000	170640	0	0	0	0
09888		无功反向（总）	智能表	413000100000 0530122741	抄表	0	0	8000	0	0	0	0	946720
有功合计									946720	0	0	0	229200
无功合计									229200	0	0	0	

仅供投标使用

9.3 提供半小时到达非部署场地的服务现场，提供专业化服务并尽快解决问题的承诺函

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

我公司提供半小时到达非部署场地的服务现场，提供专业化服务并尽快解决问题。

本公司对上述承诺的真实性负责。如有虚假，依法承担相应法律责任。

特此承诺！

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用

9.4 提供 2 条 20G 及以上速率的裸光纤政务网络接入服务能力的承诺函

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

我公司提供 2 条 20G 及以上速率的裸光纤政务网络接入服务。

本公司对上述承诺的真实性负责。如有虚假，依法承担相应法律责任。

特此承诺！

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用
AE2519CEC7C46962A8BC88EA14DB9

9.5 随时响应甲方网络安全需求（包含硬件需求），同时不增加甲方费用的承诺函

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

我公司随时响应甲方网络安全需求（包含硬件需求），同时不增加甲方费用。

本公司对上述承诺的真实性负责。如有虚假，依法承担相应法律责任。

特此承诺！

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用

9.6《南阳市政府采购供应商信用记录表》

南阳市政府采购供应商信用记录表
暨信用承诺书

2023年12月12日

单位名称	中国移动通信集团河南有限公司	统一社会信用代码	91410000719172532Q
联系人	熊永焕	联系电话	13937129955
联系地址			
信用得分	70	星级	★
信用承诺	中国移动通信集团河南有限公司自愿参加贵中心（公司）组织的本次采购活动，严格遵守《中华人民共和国政府采购法》及相关法律法规，坚守公开、公平、公正和诚实信用的原则，依法诚信经营，无条件遵守本次政府采购活动的各项规定。我们郑重承诺，本公司符合《政府采购法》第二十二条规定的条件，包括，具有独立承担民事责任的能力；具有良好的商业信誉和健全的财务会计制度；有履行合同所必须的设备和专业技术能力；有依法缴纳税收和社会保障资金的良好记录；参加政府采购活动前三年内，在经营活动中没有重大违法记录；符合法律、行政法规和采购文件规定的其他条件。如有弄虚作假或其他违法违规行为，愿承担一切法律责任，接受各级政府采购监管部门和有权机关的审查和处罚。 供应商名称（盖章）： 法定代表人（签字）： 2023年12月12日		

公共资源交易平台 南阳市政府采购供应商信用记录表 专用
AE2C19CEC77646E1A62...

9.7 提供由公安机关认证的所投政务云平台不低于三级的等保备案证明



信息系统安全等级保护
备案证明

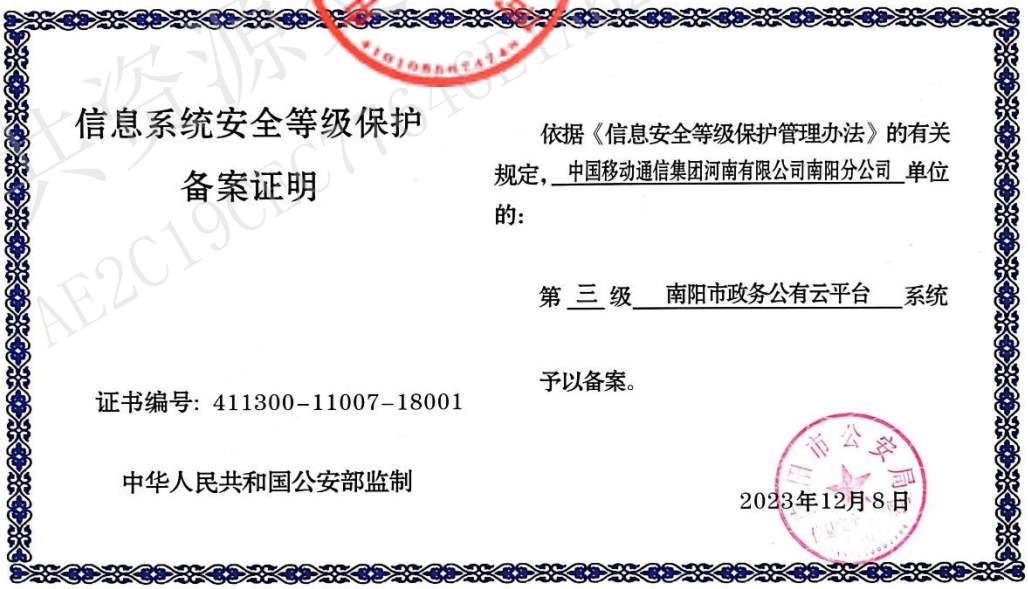
依据《信息安全等级保护管理办法》的有关规定，中国移动通信集团河南有限公司南阳分公司 单位的：

第 三 级 南阳市政务专有云平台 系统予以备案。

证书编号：411300-11007-18002

中华人民共和国公安部监制

2023年12月8日



信息系统安全等级保护
备案证明

依据《信息安全等级保护管理办法》的有关规定，中国移动通信集团河南有限公司南阳分公司 单位的：

第 三 级 南阳市政务公有云平台 系统予以备案。

证书编号：411300-11007-18001

中华人民共和国公安部监制

2023年12月8日

公共资源交易云合规专用

9.8 投标人明确 2 名主要技术负责人，且保证服务期内不更换的承诺函

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

我公司 2 名主要技术负责人为蒋纬昌和高锋杰，且保证服务期内不更换。

本公司对上述承诺的真实性负责。如有虚假，依法承担相应法律责任。

特此承诺！

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用

9.9 提供进行国产化改造、建设、替代、迁移的承诺书

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

我公司提供进行国产化改造、建设、替代、迁移。

本公司对上述承诺的真实性负责。如有虚假，依法承担相应法律责任。

特此承诺！

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

时间： 2023 年 12 月 22 日

公共资源交易平台投标专用
AE2C19CEC776...62A8BC88EA14DB9

9.10 政务云平台应通过信息安全等级保护三级认证、商用密码应用安全性评估、云计算服务安全评估的承诺书

致：南阳市政务服务和大数据管理局(采购人名称)

在贵方项目编号为 南阳政采公开-2023-111 项目名称：南阳市政务服务和大数据管理局政务云政府购买服务项目招标活动中，我公司在完全理解本项目招标的技术要求、商务条款及其他内容后，决定参与该项目的投标活动，并承诺：

我公司提供的政务云平台承诺通过信息安全等级保护三级认证、商用密码应用安全性评估、云计算服务安全评估。

本公司对上述承诺的真实性负责。如有虚假，依法承担相应法律责任。

特此承诺！

投 标 人（公章）：中国移动通信集团河南有限公司

法定代表人（负责人）或授权代表（签字）：

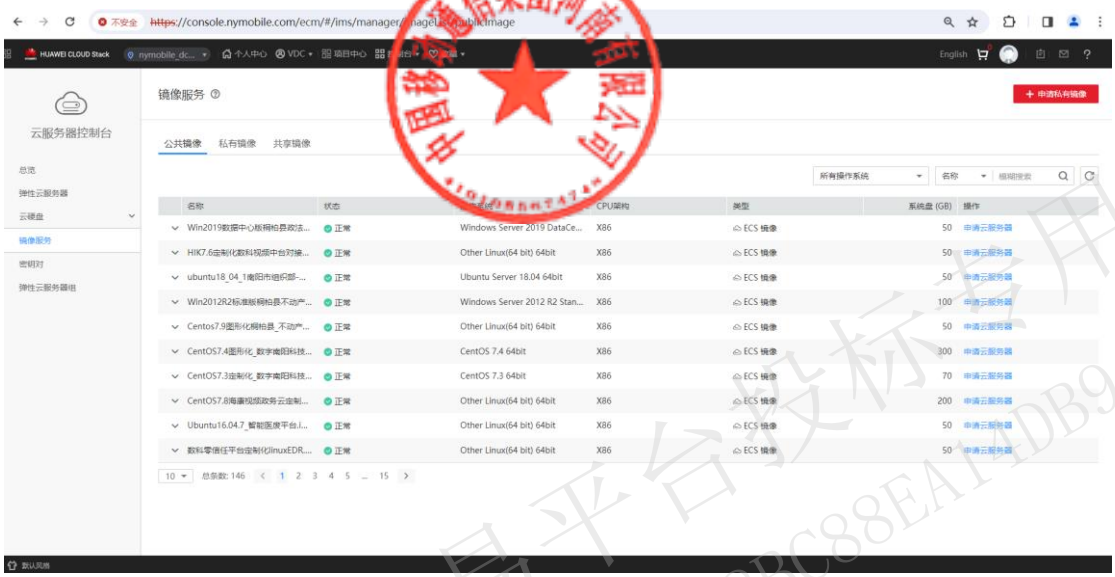
时间： 2023 年 12 月 22 日

公共资源交易平台技术专用
AE2619CE7...E1A62A8BC88EA14DB9

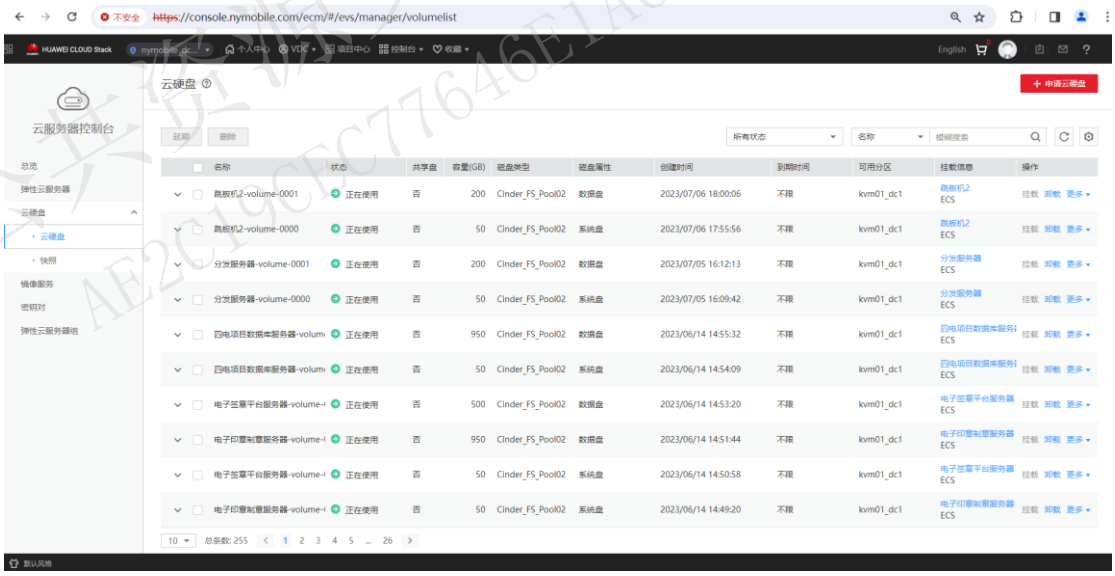
9.11 对技术要求的截图证明或证明材料

1、提供云服务器生命周期管理包括镜像与磁盘管理、安全组，提供云平台操作截图证明。

镜像

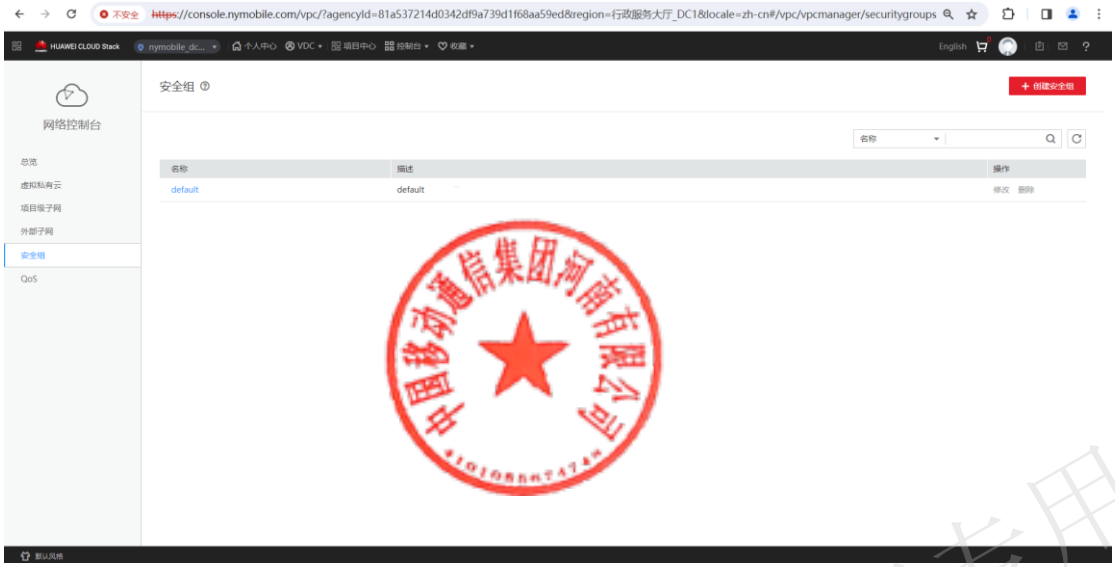


磁盘管理

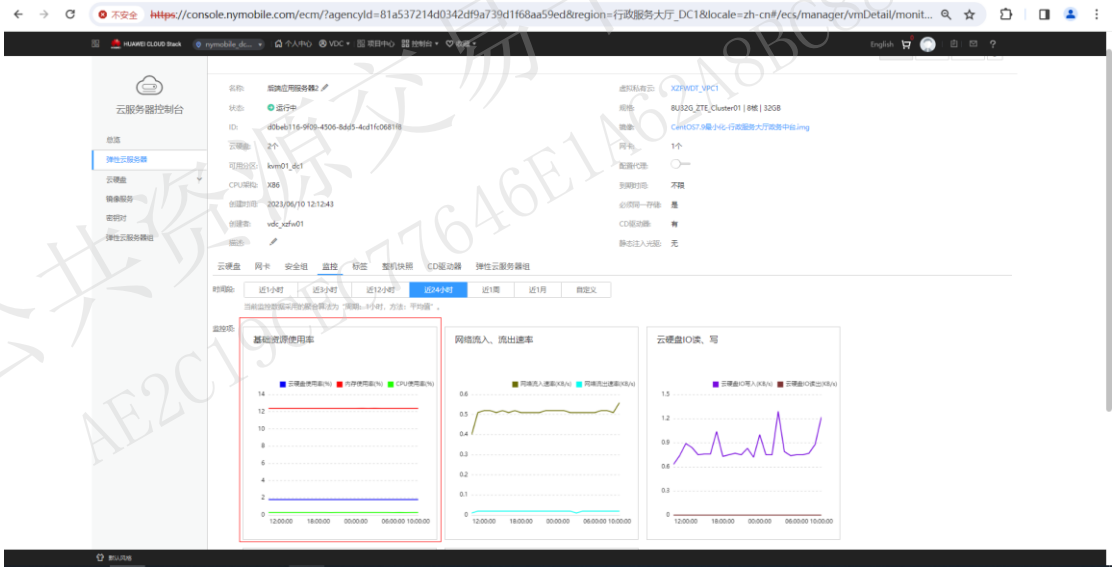


公共资源交易平台投标专用
AE2019CC77646E1A62A8BC88EA1DB9

安全组

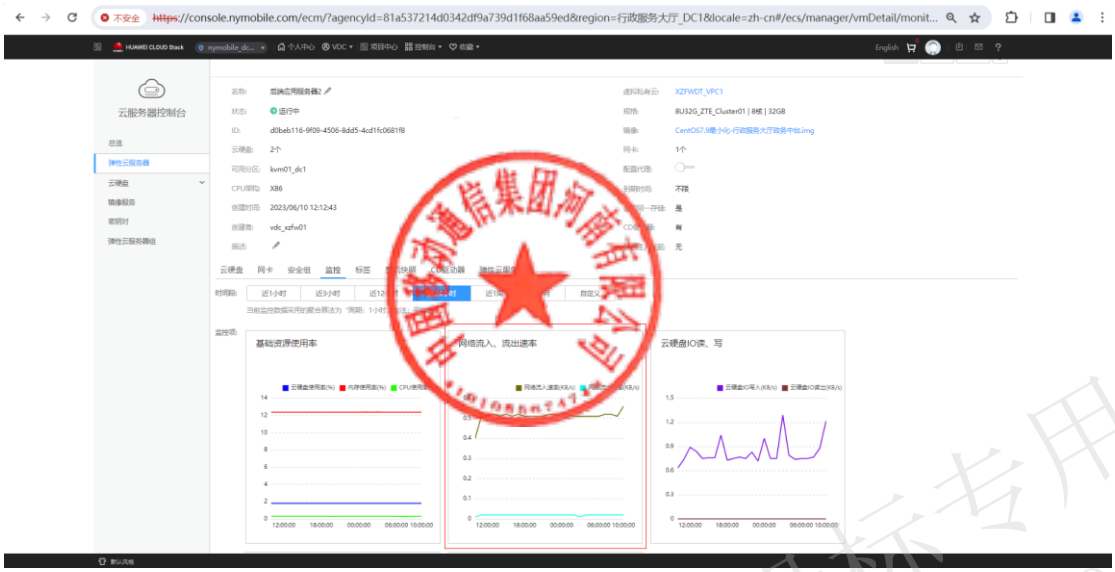


2、提供云服务器 CPU 和内存状态监控功能，监控内容包括不限于 24 小时的 CPU 利用率趋势图、内存使用率趋势，提供云平台操作截图证明；

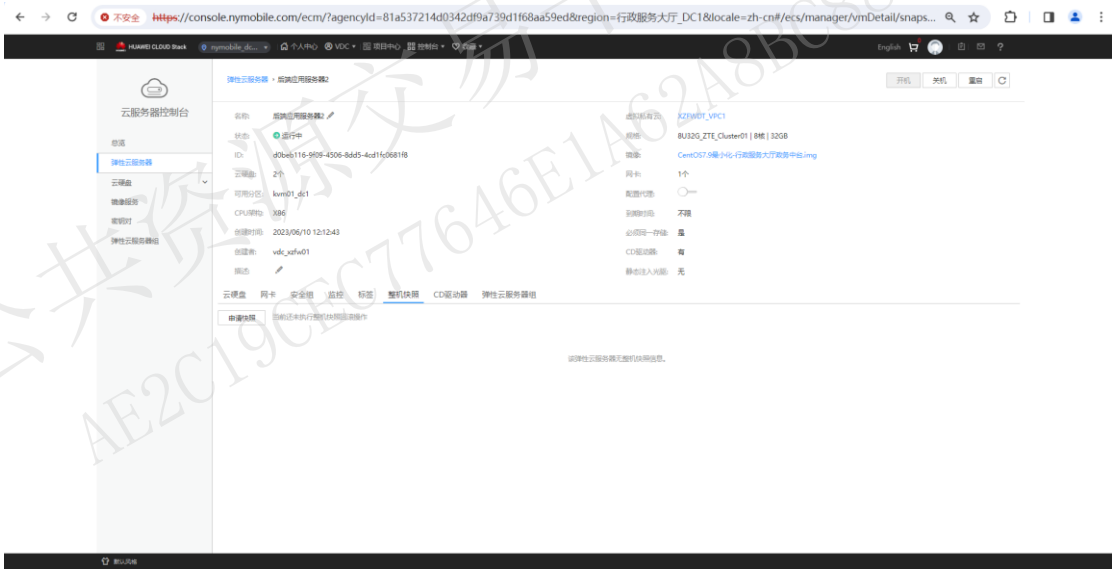


公共资源交易平台投标专用

3、提供云服务器网络监控功能，监控内容包括网络流入带宽、网络流出带宽，提供云平台操作截图证明；

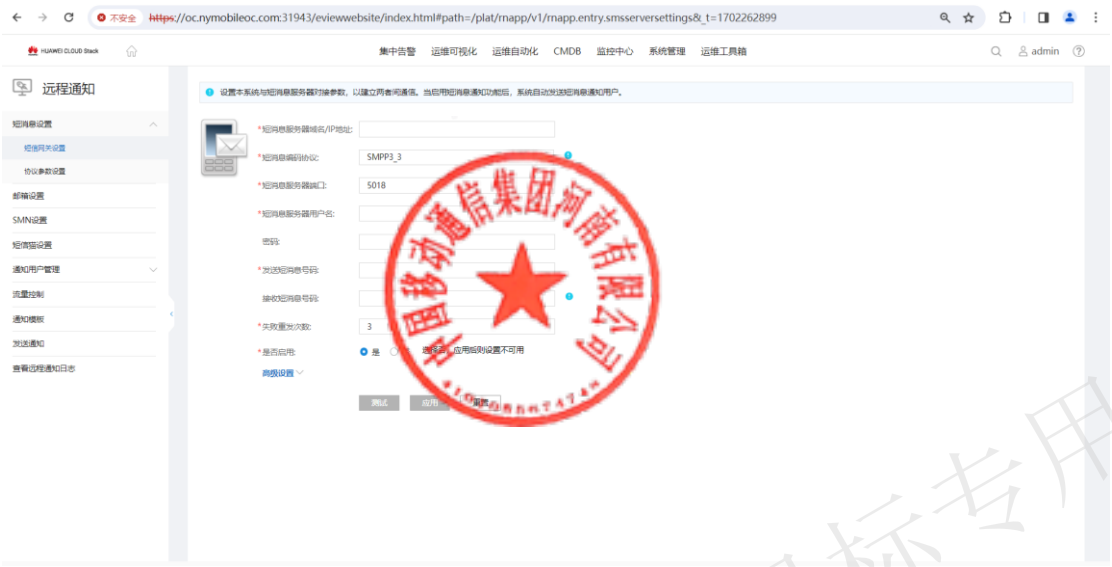


4、所使用的云平台支持云服务器快照功能，提供云平台操作截图证明。



公共资源交易平台投标专用

5、所使用的云平台支持短信、邮件告警通知，提供云平台操作截图证明。





公共资源交易平台投标专用
AE2C19CEC776461A62A8BC88EA14DB9

6、云主机（ECS）可用性≥99.99%，提供相关证明材料。



7、块存储（云硬盘）和对象存储数据存储持久性≥ 99.9999%，提供提供相关证明材料。



公共资源交易平台技标专用
AE2C19CD77C46E1A6218BC88EA14DB5



8、云数据库业务可用性满足基本要求且≥99.99%，云数据库的数据存储持久性≥99.9999%,提供相关证明材料。



公共资源交易平台投标专用
AE2C19CC7C6C4E62A8BC88EA14DB9