云运维保障方案（完整版）

公司名称：北京乘云至达科技有限公司

目录

1、运维项目

1.1监控服务

提供 7*24 小时的监控服务，包含系统层次监控服务、阿里云资源监控、应用层监控服务服务。具体如下：

- 基础监控 CPU、内存、磁盘、网络等；
- 中间件性能监控（总中间件数量包含 50 个，比如 5 台上都安装了 tomcat 算作
  5 个）：
  *Apache（需在 httpd.conf 中添加 location 并重启服务）；
  *Tomcat（需在 catalina.sh 中添加 jmxremote 并重启服务）；
  *Nginx（需在 nginx.conf 中添加 server 并重启服务）；
  *MySQL（需要执行 status、extended-status 的权限）；
  *MongoDB（需要执行 db.serverStatus()的权限）；
  *Redis（需要执行 info 的权限）；
  *ZooKeeper（需要执行 stat 的权限）；
  *php-fpm（需在 php-fpm.conf 中开启 fpm-status，在 Nginx 中添加 location并重启服务）；
- 端口监控（包含 80 个）；
- 5 个URL 监控（每个 URL 提供 3 个监测点）；
- 日志文件关键字监控（包含 10 个关键字和 10 个日志文件）；
- ECS、RDS、SLB、OSS 的性能和过期时间监控（一个阿里云账号，需要 AK 信息）。
- 其他自定

义监控例：监控

监控模板内容					
监控说明：				■需要监控 □ 无需监控	
基础监控：					
监控内容	■CPU	■Memory	■Network	■Disk	■OS
其他：	填写额外的监控内容				
应用程序监控：					
WEB：	□ IIS	□ Apache	■Nginx	■Tomcat	□ Resin

数据库：	☐ MySql	☐ MSSQL	☐ Oracle	☐ MongoDB	■Redis
	☐ Memcached	■RDS-Mysql	■RDS-MSSQL	☐ KVStore	■ zookeeper
其他：	ehcache 监控，Solr 监控				
Port 监控：					
监控内容:	■80	■22	☐ 3306	☐ 1433	☐ 21
其他：	*8081, 8086. 8093, 8088, 8089, 6379, 2181, 8093*				
URL 监控：					
监控内容:	☐ https	■http	■api		
URL:	api 接口				
自定义监控	error 日志报警				

例：监控报警的规则如下：

No	分类 1	分类 2	监视间隔(分)	监视间隔（分）异常时	Alert 邮件送信时机
1	OS 运行监视	zy_agent ping 监视	1	1	异常时，每 1 分钟 check 一次，5 次之后还是异常则发信
2	性能监视(OS 系)	CPU 使用率监视(%)	1	1	
		CPU Run Queue 监视 (Load Average)	1	1	
		空 Memory 率（%）	1	1	
		空 Swap 领域监视(%)	无	无	可以根据需求设定
3	Disk 使用率监视(OS 系)		1	1	异常时，每 1 分钟 check 一次，1 次之后还是异常则发信
	Disk IO（OS 系）	磁盘读写监控和读写速度监控	1	1	每 1 分钟检查一次，5 分钟内的平均值大于 20%则发信
	进程数监视(OS 系)	主机运行的进程数监控	1	1	每 1 分钟检查一次，5 分钟内的平均值大于 300 则发信

4	Process 监视（OS 系）		1	1	每 1 分钟 check 一次，3 次之后还是异常则发信

5	Port 监视		1	1	每 1 分钟 check 一次，3 次之后还是异常则发信
6	Log 监视		1	1	主动监控关键字，出现关键字则发信
7	URL 监视		2	2	监控反馈状态，当返回值不为 200 则发信
8	RDS 监视	CPUUtilization	5	1	每 5 分钟 check 一次，3 次之后还异常则发信
		DatabaseConnections	5	1	每 5 分钟 check 一次，一发现异常则发信
		IOPS	5	1	每 5 分钟 check 一次，一发现异常则发信
9	文件删改监视		1	1	一发现异常即可送信

1.1.1 系统监控内容

- 系统进程、主机名、密码更改等系统状态监控：监控*.conf 文件变动,iptables 状态，运行进程数。
- CPU、磁盘、内存、网卡等系统性能状态监控：CPU 使用率，CPU Load,内存使用率，网络出入网流量，磁盘使用空间，磁盘 IO。
- 中间件（如 Nginx、Tomcat、Apache、Weblogic 等），应用程序状态/服务进程、日志文件、应用状态等监控。

例：中间件监控如下：

1.Tomcat 监控项目	
监控内容	监控内容解释
Tomcat version	Tomcat 的版本
Tomcat-堆内存已使用	Tomcat 目前已经使用的内存
Tomcat-堆内存已提交	Tomcat 配置文件中的最小内存
Tomcat-堆内存最大	Tomcat 配置文件中的最大内存
Tomcate-http-bio-80-bytesReceived	tomcat bio 接收数据量
Tomcate-http-bio-80-bytesSen	tomcat bio 发送数据量
Tomcate-http-bio-80-errorCount	tomcat bio 错误统计
Tomcate-http-bio-80-requestCount	tomcat bio 请求次数统计
Tomcate-http-bio-80-当前线程数	tomcat bio 申请线程数
Tomcate-http-bio-80-最大线程数	tomcat bio 线程总数
Tomcate-http-bio-80-繁忙线程数	tomcat bio 使用线程总数
Tomcat-http-80 活动线程	tomcat 使用的线程数据
Tomcat-http-80 线程峰值	tomcat 使用的最大线程数
Tomcat-http-80 线程总计	tomcat 线程数总量

Tomcat-Sessions-当前活动**会**话**数**	Tomcat 的会话情况
Tomcat-Sessions-最大活动**会**话**数**	Tomcat 的会话情况
Tomcat-Sessions-会话数	Tomcat 的会话情况
2.Nginx 监控项	
监控内容	监控内容解释
nginx.accepts	nginx 的 accepts 数
nginx.active	nginx 的 active 数
nginx.handled	nginx 的 handled 数
nginx.reading	nginx 的 reading 数
nginx.requests	nginx 的 requests 数
nginx.waiting	nginx 的 waiting 数
nginx.writing	nginx 的 writing 数
3. Redis 监控项	
监控内容	监控内容解释
port 6379 is listening	端口状态
redis connected_clients	已经连接的客户端数量
redis keyspace_hits	查找数据库键成功的次数。
redis keyspace_misses	查找数据库键失败的次数。
redis total_commands_processed	服务器已执行的命令数量。
redis total_connections_received	服务器已接受的连接请求数量。
redis uptime_in_days	持续运行时间
redis used_memory	内存总量
redis used_memory_peak	内存消耗

1.1.2 阿里云资源监控内容

- 阿里云资源 ECS/SLB/RDS/OSS 异常及其它云服务等相关监控：通过调用阿里云相应资源的 API，获取监控和报警数据展现在云管监控平台，并反馈通知客户。
- 资源过期监控预警：对于已经提供资源过期 API 的资源，例如 ECS 等产品，通过 API 调取资源过期时间，在资源到期之前通过监控平台告知反馈客户。
- 云资源相关升级/变

更监控。例：阿里云资源监

RDS for MySQL 监控项	
监控内容	监控内容解释
MySQL_COMDML_com_delete	平均每秒 Delete 语句执行次数
MySQL_COMDML_com_insert	平均每秒 Insert 语句执行次数

MySQL_COMDML_com_insert_select	平均每秒 Insert_Select 语句执行次数
MySQL_COMDML_com_replace	平均每秒 Replace 语句执行次数
MySQL_COMDML_com_replace_select	平均每秒 Replace_Select 语句执行次数
MySQL_COMDML_com_select	平均每秒 Select 语句执行次数
MySQL_COMDML_com_update	平均每秒 Update 语句执行次数
MySQL_InnoDBBufferRatio_ibuf_dirty_ratio	缓冲池脏块的百分率
MySQL_InnoDBBufferRatio_ibuf_read_hit	缓冲池的读命中率
MySQL_InnoDBBufferRatio_ibuf_use_ratio	缓冲池的利用率
MySQL_InnoDBDataReadWriten_inno_data_read	平均每秒钟读取的数据量
MySQL_InnoDBDataReadWriten_inno_data_written	平均每秒钟写入的数据量
MySQL_InnoDBLogWrites_Innodb_log_writes	平均每秒向日志文件的物理写次数
MySQL_InnoDBLogWrites_Innodb_log_write_requests	平均每秒日志写请求数
MySQL_InnoDBLogWrites_Innodb_os_log_fsyncs	平均每秒向日志文件完成的 fsync()写数量
MySQL_IOPS	IOPS 使用量
MySQL_MyISAMKeyBufferRatio_Key_read_hit_ratio	MyISAM 平均每秒 Key Buffer 读命中率
MySQL_MyISAMKeyBufferRatio_Key_usage_ratio	MyISAM 平均每秒 Key Buffer 利用率
MySQL_MyISAMKeyBufferRatio_Key_write_hit_ratio	MyISAM 平均每秒 Key Buffer 写命中率
MySQL_MyISAMKeyReadWrites_myisam_keyr	MyISAM 平均每秒钟从硬盘上读取的次数
MySQL_MyISAMKeyReadWrites_myisam_keyr_r	MyISAM 平均每秒钟从缓冲池中的读取次数
MySQL_MyISAMKeyReadWrites_myisam_keyr_w	MyISAM 平均每秒钟从缓冲池中的写入次数
MySQL_MyISAMKeyReadWrites_myisam_keyw	MyISAM 平均每秒钟从硬盘上写入的次数
MySQL_QPSTPS_QPS	平均每秒 SQL 执行次数
MySQL_QPSTPS_TPS	平均每秒事务数
MySQL_RowDML_Inno_log_writes	平均每秒向日志文件的物理写次数
MySQL_RowDML_inno_row_delete	平均每秒从 InnoDB 表删除的行数
MySQL_RowDML_inno_row_insert	平均每秒从 InnoDB 表插入的行数
MySQL_RowDML_inno_row_readed	平均每秒从 InnoDB 表读取的行数
MySQL_RowDML_inno_row_update	平均每秒从 InnoDB 表更新的行数
MySQL_Sessions_active_session	当前活跃连接数
MySQL_Sessions_total_session	当前总连接数
MySQL_MemCpuUsage	CPU 利用率

SLB 监控项	
监控内容	监控内容解释
PacketTX	端口每秒流出数据包数
PacketRX	端口每秒流入数据包数
TrafficRXNew	端口每秒流入数据量
TrafficTXNew	端口每秒流出数据量

ActiveConnection	端口当前活跃连接数，既客户端正在访问 SLB 产生的连接
InactiveConnection	端口当前非活跃连接数，既访问 SLB 后未断开的空闲的连接
NewConnection	端口当前新建连接数

1.1.3 应用监控

HTTP/TCP 全国或世界监控节点访问应用或主机的可用率、延时状态监控（默认全国节点），缺省配置是 3 个URI 监控地址

- 网站首页或其他应用地址监控（默认首页）。
- API 接口监控（需要用户提供 API 接口）。
- 模拟用户登录、查询等应用监控（需要用户提供 api 接口）。

1.1.4 容器监控

容器的监控指标主要为 Docker 容器资源监控。各监控具体细项如下：

Docker 容器资源	
监控内容	监控内容解释
CPU Usage	容器 CPU 的利用率
Total Memory	容器内存大小
Memory Usage	容器内存使用大小
Memory_Percent	容器内存使用百分比
Network Traffic(Inbound)	容器网卡进流量
Network Traffic(Outbound)	容器网卡出流量
Read IOPS	容器读 IOPS
Read IOPS	容器写 IOPS

1.2应急事故处理服务

包含系统异常处理、应用异常处理、阿里云相关异常处理。发现监控报警，运维人员立即上线就位处理事故。若发现异常事故是由于客户应用程序导致，需根据约定邮件或电话通知客户处理。

1.2.1 系统异常处理内容

- 系统进程、主机名、密码更改等状态异常处理。
- cpu、磁盘、内存、网卡状态异常处理。
- 中间件、服务进程、相应服务状态异常处理。
- 通过脚本扩展的自定义的监控项状态异常处理。

1.2.2 阿里云资源相关异常处理

- 宕机迁移、RDS 异常及其它云服务等相关事故异常处理。
- 云服务相关升级期间导致服务异常中断异常事故处理。

1.3日常运维服务

包含环境设置、安装部署、数据迁移、中间件参数调配、数据备份、升级/变更资源等操作。

1.3.1 阿里云资源运维

- 基于客户要求，进行阿里云资源升降配操作
- 协助 ECS、RDS、OSS 配置的选型与初始化
- 协助设置安全组，SLB（公网或私网负载均衡）
- 协助 VPC 专有网络设置

- 按客户要求，为应用程序服务器设置 NAT 网关来访问互联网以提供 Web 服务调用和外网访问
- 云上 VPN 网关、高速通道的技术支持，如果涉及到线下的 VPN 设备、专线连接设备需要客户联系设备供应商协助
- 设置用户/角色 - RAM
- 创建镜像，这将有助于在不同地理区域上快速部署多个测试或生产环境

1.3.2 备份运维服务

- 按客户需求，在阿里云平台配置云服务器快照策略
- 按客户需求，在阿里云平台配置云数据库备份策略
- 提供其它备份工具及备份建议

1.3.3 其他通用运维服务：

- 为客户提供阿里云服务降升级或停机公告
- 协助阿里云平台问题根本原因分析
- 建议阿里云平台所有操作的记录方式

1.4安全运维服务

提供系统安全运维加固，应用安全扫描，安全事故处理。

1.4.1 运维安全加固

针对客户业务应用，进行系统层次、应用层次、网络层次的安全加固，对安全组和主机对外端口进行设置。

- 服务器账号分级权限管理
- 和客户确认后，关闭部分不常用端口
- 限制 root 权限的使用
- 修改 SSH 默认端口
- 密码随机化加固
- 部署 cmd_track 安全小工具，记录用户命令操作明细（包括用户、时间点、路径、命令明细等）
- 添加用户登陆警告信
- 防火墙脚本进行安全加固，限制外网登陆 ip

1.4.2 补丁管理/安全警报

- 基于阿里云安骑士或云盾平台建议，应用操作系统安全级别补丁
- 漏洞分析和应用修复补丁
- 包括无限制的一次性补丁和安全警报。

- 所有补丁程序在执行前将进行补丁分析，补丁文档将被审查，所有先决条件将被识别。 所有将需执行的补丁将按照顺序一一执行。 客户将负责决定是否执行补丁程序。
- 北京乘云安全团队和客户将制定一个发布管理规程，任何部署到各种实例的补丁
/自定义配置必须经过客户管理部门完全接受和批准。在任何情况下，北京乘云团队都不会将补丁程序/自定义配置直接应用到没有至少在一个额外实例（例如开发或测试实例）来先行执行补丁程序的生产实例。
- 所有补丁执行后的功能测试是客户的责任。 补丁申请将以符合标准操作程序的方式进行，标准操作程序应由客户书面规定和批准。
- 重要补丁更新将在每个季度进行一次审核，由于这些更新是由阿里云发布的,客户会被告知取内容和补丁要求。

1.4.3 应用安全扫描

提供应用安全扫描的建议与实施方案，包括：

- 阿里云态势感知安全监测、云安全中心检测、DDOS 防护（需要客户支付阿里云安全产品费用）

1.5网络服务

包含 VPC 规划服务，VPN 隧道调试服务，VPN 故障排除服务，提供专线咨询服务

1.5.1 VPC 规划服务

- VPC 网段的规划、创建服务；
- VPC 路由调整服务；

1.5.2 VPN 隧道调试服务

- VPC 环境下的 VPN网关 配置服务

- 金融云 VPC 环境下的 IPSEC 配置服务

备注：为客户提供的 VPN 隧道配置服务，仅包括阿里云上的 flexgw 安装、配置，涉及到客户线下设备配置由客户配置，北京乘云将会在整个 VPN 调试过程中配合客户完成本次VPN 的调试。

1.5.3 VPN 故障排除服务

- 阿里云上 FlexGW 的日志分析、故障排查
- 阿里云上和 VPN 相关的网络分析
- 协助分析客户侧 VPN 问题

1.5.4 提供专线咨询服务

- 承接客户与运营商之间的专线安装的沟通工作，确保专线从客户端到阿里云端正常开通；
- 调试阿里云端专线的路由配置，确保阿里云端到客户侧的路由配置正常；
- 协助客户调试线下路由，确保客户侧路由到阿里云端路由配置正常；
- 协同客户一起对线下和线下网络进行联通性测试，完成本次专线施工

1.6数据库服务

包括数据库安装、迁移、升级、备份恢复、故障处理、高可用性解决方案及性能优化等方面的服务。数据库类型包括 MySQL 、SQL Server 、PostgreSQL 等及 RDS 各类型数据库。

- 阿里云上的云数据库（RDS，MongoDB，Memcache，Redis 等或 ECS 上自建的上述数据库）7x24 监控和响应
- 主流数据库（Sqlserver，Mysql，MongoDB，Memcache，Redis等） 安装、配置及技术支持
- 定义和实施有关配置的最佳实践
- 基于阿里云平台监控云数据库-主动监控和事件通知（长时间运行的查询，死锁，数据库连接池，tmp 文件）
- 索引的添加、更改或删除建议
- 备份和恢复的计划与建议
- 提供 HA 配置支持
- 克隆实例：生产实例到非生产实例
- RDS 升级方案建议及实施

- 按需定期提供慢查询 SQL 语句
- 数据库用户创建/删除（按客户要求）
- 按需调整数据库实例配置

1.6.1 安装配置服务

- 配合用户在指定的系统上安装数据库软件
- 正确安装和配置数据库系统必须的依赖环境
- 设置合理参数、字符集、用户、数据文件
- 撰写数据库系统安装报告

1.6.2 数据库系统升级

- 确定数据库系统升级版本
- 介质的准备或协调
- 升级实施步骤的测试及准备
- 升级实施

1.6.3 备份与恢复

采取物理备份与逻辑备份相结合的备份方式对数据库进行备份，并定期做数据库的恢复演练，确保所有的备份是可用的。

- 设置自动备份策略：保留天数、备份周期、备份时间、日志备份
- 设置手动备份：选择备份方式、备份策略
- 覆盖性恢复：指定备份集的数据恢复到当前实例上
- 备份集恢复：指定备份集的数据恢复到一个过期时间为 N 天的临时实例上
- 时间点恢复：选择临近时间点，系统根据全量备份以及之后的日志备份，将数据重放到一个过期时间为 N 天的临时实例上

1.6.4 故障处理

- 对数据库系统的故障进行快速准确定位
- 排除数据库系统故障
- 撰写故障分析报告，描述故障产生的原因、解决办法、避免发生同样故障的措施

1.6.5 数据库监控

提供数据库的监控，数据库的监控包括：

- 监视数据库系统资源的使用情况，包括 CPU、内存、IO 的状况
- 监视数据库系统日志等情况
- 查看数据库系统进程状况
- 撰写性能监控及分析报告
- 设置监控频率：控制台 300 秒/次、zabbix120 秒/次
- 设置报警规则：统计周期 5 分钟，连续出现 3 次超过阈值后报警
- 设置通知对象：控制台报警发送短信通知、截图发至钉钉
- 设置监控视图：数据库类型、监控实例、

监控项例：监控列表如下：

数据库类型	监控项
MySQL	磁盘空间、IOPS、连接数、CPU使用率、网络流量、QPS/TPS、InnoDB缓冲池、InnoDB读写次数、InnoDB日志、临时表、MyISAM Key Buffer、MyISAM读写次数、COMDML、ROWDML
SQL Server	连接数、缓存命中率、平均每秒全表扫描数、每秒SQL编译、每秒检查点写入Page数、每秒登录次数、每秒锁超时次数、每秒死锁次数、每秒锁等待次数、网络流量、QPS\TPS、CPU使用率、IOPS、磁盘空间
PostgreSQL	磁盘空间、IOPS
RDS for PPAS	磁盘空间、IOPS

1.6.6 数据库系统参数调整与优化

- 数据库系统配置优化
- 涉及业务层面的 SQL 语句优化调整，需要客户开发人员协同解决。
- 数据库系统参数调整

1.6.7 数据库系统迁移

针对数据库系统的迁移、测试服务，包括：

- 迁移本地数据库（MySQL/SQL Server/PostgreSQL 等）到 RDS 对应版本
- 迁移 RDS 数据到本地 MySQL、SQL Server、PostgreSQL 等

1.7季报/故障报告服务

记录系统状态及变更信息，以及日常运维内容以北京乘云运维报告平台的形式定期提供给用户。

作为云托管运维服务的组成部分，北京乘云将在约定的时间间隔提交以下交付物。 这些可交付成果的格式、内容和时间表可以在项目启动阶段与客户协商后进行修改。

1) 总结(季报)
   - 季总结报告
2) 事件报告（季报）
3) 安全报告(季报)
   - 主机安全
   - 漏洞
4) WEB报告(季报)
   - URL 监控
5) 主机报告(季报)
   - 基础监控
   - 端口监控
6) 数据库报告(季报)

2、服务水平协议SLA 责任和假设 日常运维服务

2.1 服务水平协议 SLA

北京乘云在运维服务过程中将按监控报警发现的问题类型和严重程度，采用分阶段的渐进式问题跟踪、升级和处理策略，并向客户指定的团队报告。 问题分为以下四个类别，响应时间定义如下表 1 所示。

以下政策仅适用于北京乘云的“日常云运维服务”。阿里云官方产品和服务请参考相应阿里云官网 SLA.

表 1 注释

客户通过北京乘云服务入口提交事件（或“问题”），从而分配一个严重性级别。事件的定义是客户认为需要北京乘云重点审查的任何系统操作故障或异常情况。事件必须使用北京乘云提供的服务入口进行提交，或者紧急情况下可先通过电话沟通。客户可以随时在北京乘云服务入口提交事件或请求。这些事件或请求可能会经过双方的技术审查或决议后被升级为故障。 注：事件仍以 15 分钟内响应为准。

表 1 - 服务级别和严重性定义

严重性	业务影响	定义	响应	决议/处理	客户责任
1	灾难 (Disaster)	这类问题会导致由于系统服务（非阿里云层次问题、非业务代码问题）全面崩溃，业务因此不能有效持续，对业务来说是灾难性的。	5 分钟内响应	7 X 24 小时处理直到问题解决	需要指定 7*24 主要和次要联系人
2	严重 (High)	这类问题会导致严重的服务中断情况。出现系统部分或小范围功能失效但系统仍可在受限状态（性能下降）下能继续运行，业务仍能持续开展。	15 分钟内响应	7 X 24 小时直到给出解决方案	按需需要立即响应和回应

3	一般 (Average)	这类问题会导致不太严重的服务中断或一个不严重的故障或问题，但业务系统能继续运行且性能不受影响。必须通过手动操作来解决并恢复。	30 分钟内响应	5 X 8 小时	按需在 48 小时内响应和回应
4	警告 (Warning)	这类问题不会导致服务的中断。 一般可以通过手动操作来处理。	30 分钟告警，24 小时内技术工程师响应	5 X 8 小时	按需在 48 小时内响应和回应

问题升级方案

为了确保此处服务水平定义的响应和处理要求，北京乘云将采用分层问题跟踪、升级和处理流程，其中始终会包含第一响应者和第二响应者，以及问题升级时对应的响应者经理或代理经理。 北京乘云将向客户提供响应者联系信息，问题响应及升级联系信息如果出现任何更改，将在两个工作日内以正式形式通知客户。

2.2 客户责任

为了圆满地完成本工作说明书所定义的工作，北京乘云必须依靠客户的合作和支持。 特别是，客户将负责以下操作或提供先决条件：

1 客户应指定和明确第一对接人以及第二对接人（备用），负责协调所有与客户有关的活动，并作为与北京乘云沟通的联络接口人，根据需要协助双方之间的问题。当第一对接人不在时，第二对接人将作为联络接口人。 对接人将：
   a. 作为客户内部部门和北京乘云团队之间的接口；
   b. 根据需要安排所有系统管理必要的许可和访问权限，包括访问代码，密码和任何现场资源所需的证件。
2 北京乘云的用户在云账号下须有一台单独的机器作为运维管理服务器，在该机器上安装监控代理程序等，该机器配置为 8c16g 且可访问公网。
3 客户应负责客户网络内的所有网络基础架构和配置以及对阿里云环境的防火墙 / VPN 访问。
4 客户应负责应用测试和系统间功能的集成测试与验证，并指派必要的开发人员和 IT 人员完成项目计划中所述的工作。
5 客户应承担在实施本“工作说明书”中产生的软件许可，网络和计算基础设施费用相关的成本，除非在此包含在服务范围内的。
6 客户应负责由于从本地迁移到阿里云环境可能产生的应用程序修改（例如：是否在应用程序中存在硬编码的 IP 寻址/文件共享）。

2.3 假设

为了支撑本服务内容，北京乘云做出了以下关键假设：

1 本提案中的服务范围以工作说明书中列出的工作任务为基础。服务范围之外的任何其他工作任务可能会产生额外费用，需要进行合同变更。

2 设定通用的电子邮件 ID（例如，123@cloudcy.cn）。 所有的电子请求都会发送到这个电子邮件 ID。

3 提供专用电话号码用于阿里云托管技术服务台。该电话服务 7*24 小时可用并将呼叫转移给适当的服务顾问或服务经理接听。

4 本方案仅面向本项目报价清单中所包含数量的阿里云公有云产品的运维。

3、运维规范

3.1 安全规范

甲方给到乙方代维的对应服务器，需要严格遵守本运维服务规范。如若不按照此规范而产生的对应运维安全事故，相应责任需由相关方承担。

甲方和乙方所有人员对运维资源的管理都以堡垒机作为入口，操作记录全部被记录下来， 便于审计和记录。

3.2 账号规范

3.2.1 运维账号

乙方统一采用 cyadmin 用户登录服务器进行运维操作。

甲方统一采用 xxadmin 用户登录服务器进行日常操作，不需要有 root 权限。

3.2.2 控制台账号

甲方需要为乙方提供两个阿里云控制台账号。

一个账号供乙方登录甲方的阿里控制台，该账号需要甲方根据实际情况分配对应的权限。另外一个账号需要甲方授予该账号只读访问所有阿里云资源的权限（ReadOnlyAccess），并为该账号创建 AccessKey，将该账号的 AccessKey 提供给乙方，方便乙方为甲方部署监控、提供季报等场景中使用。

名词解释：

RAM (Resource Access Management) 是阿里云提供的资源访问控制服务。通过 RAM，您可以集中管理您的用户（比如员工、系统或应用程序），以及控制用户可以访问您名下哪些资源的权限。

AccessKey（AK，访问秘钥）相当于登录密码。AccessKey 用于程序方式调用云服务 API， 您可以使用 AccessKey 构造一个 API 请求（或者使用云服务 SDK）来操作资源。AccessKey 包括 AccessKeyId 和 AccessKeySecret。AccessKeyId 用于标识用户。AccessKeySecret 是用来验证用户的密钥。

3.3 服务对接规范

- 甲方需为本运维服务合同指定一名主要接口人以及至少一名次要接口人。接口人联系方式包括电话和邮箱。
- 乙方需为甲方指定运维项目负责人、运维工程师等接口人。接口人联系方式包括电话和邮箱。
- 甲方以在北京乘云指定服务群发起提交服务需求，乙方工程师接收事件并审核通过后
  ，可处理甲方服务需求。
- 若甲方人员服务需求涉及威胁系统安全或影响甲方业务运转，乙方需向甲方给出警示提醒且有权拒绝甲方请求。若甲方人员执意执行此类请求，需由甲方的服务联系人出具书面或邮件确认书，乙方可按照甲方要求执行，但乙方不承担由此带来的任何经济和法律责任。
- 甲方负责业务代码层次的更新发布、异常解决、bug修复等问题，关于业务代码层次的需求，需要以甲方为主。

3.4 监控事件服务流程

乙方在甲方系统异常的时候，需以消息推送/电话的方式 7*24 的通知到甲方。当甲方出现核心业务异常不能正常访问、服务器宕机等这样灾难性的事故时，乙方在默认情况下，会 7*24 的电话通知客户及事故处理情况。低于此类的事故级别，乙方会以消息推送的方式通知。具体的通知的时间，通知的方式可以由双方协商确定。

3.5 变更规范

3.5.1 新增资源

甲方新增服务器或者数据库运维范围，需要在北京乘云服务群进行通知，乙方根据事件内容对资源进行安全加固、监控部署等操作。

3.5.2 配置变更

甲方有配置变更需求，需要在北京乘云服务群授权乙方工程师对服务器进行变更操作。乙方在变更操作之前需要将变更可能造成的风险告知甲方并得到甲方的确认。

变更操作之前乙方需要进行充分的测试，且不能在甲方线上环境进行测试及调试,如若重要　测试需要测试环境，需要甲方提供，否则不予变更。

变更操作前乙方需要对服务器或配置文件进行备份。

3.6 季报规范

乙方需在每季度前为甲方提供上季度的总结报告并以邮件方式通知到甲方，季报包含概览、事件报告、安全报告、web 报告、主机报告、数据库报告等内容。