目录

1. 工作说明书 – Cloud Maintenance MSP运维版

本 Cloud Maintenance MSP 运维版工作说明书（以下简称“本工作说明书”或 “SOW”）作为杭州济通科技斯法科技有限公司（以下简称“济通科技”）和_____公司（以下简称了“客户”）在_____日期_____签署的技术服务合同（以下简称“合同”）的补充说明。 如果本工作说明书与上述合同存在不一致或冲突之处，应以本工作说明书为准。除此之外，合同将继续保有全部的法律效力。

1.1 工作和服务声明

根据合同中规定的条款，济通科技同意按照本工作说明书提供云托管运维服务。

1.2 工作地点说明

Cloud Maintenance MSP服务团队主要集中在杭州，原则上采用远程方式进行服务支持。

1.3 云方案架构师/顾问资源说明

Cloud Maintenance 架构师团队支持国内主要一线城市（杭州、上海、北京、广州等）的现场咨询服务。基于客户需要，支持电话会议，视频会议，客户现场讨论等形式。

1.4 定价及费用说明

本工作说明书以客户实际使用的阿里云资源种类和数量为基数进行工作量及资源使用的定价。

合同项目费用包含服务周期内的阿里云资源使用费用和云托管运维服务费用。

客户使用的其它第三方商业/付费软件 license 费用，技术支持费用需要客户自行承担。

阿里云资源费用说明

- 阿里云资源费用是指在阿里云使用各种资源（如云服务器，块存储，快照，云数据库，网络带宽，VPN，弹性 IP，云安全等）每小时的使用费用。
- 实际使用成本将根据使用情况和配置的资源数量而有所不同。阿里云可能随时调整云资源的费用，但客户不能因以前由济通科技开具的资源费用而追溯任何价格变动。

2. 云托管运维服务

Cloud Maintenance MSP 运维版将为客户的阿里云托管平台提供下述管理及服务，作为云托管运维服务的组成部分。

2.1 运维管理规范

1. 安全管理
   - 最佳云安全实践，及时响应安全事件，执行和维护整个服务周期，根据双方约定，包括但不限于安全组，网络ACL，云防火墙，云WAF,云安全中心。
   - 配置和授权阿里云RAM帐号管理员访问各种阿里云资源。
   - 协助客户处理解决云安全中心的阿里云平台事件通知。
2. 性能管理
   - 定期检查云监控及关键指标，监测阿里云资源性能并提供建议。
   - 协助客户运维团队和客户供应商支持团队实施客户批准的变更。
3. 费用管理
   - 跟踪客户阿里云帐户各种资源的使用情况并设置报警监控异常行为，以通知相应的团队采取纠正措施。
   - 持续跟踪阿里云关于新服务发布和降价情况的最新公告，并向运维团队建议相关变更
   - 根据客户云上资源情况结合最佳实践提供费用优化方案
4. 自动化
   - 识别关键活动自动化的机会，并使用客户许可的工具来实施这些自动化方案。
   - 协助客户团队使用阿里云API或SDK准备所需的自动化脚本。
   - 提供工具来自动执行与云平台管理相关的所需任务，例如制作快照，停止/启动服务器等。
5. 变更管理
   - 使用阿里云操作审计服务监控变更并汇报任何可疑活动。
   - 采用客户接受的变更管理流程实施客户账户上的任何变更。

- 提供统一云服务管理平台记录并审批云服务商、软件服务商发起的变更请求，并对应到资产进行存档供用户查阅。

6. 从客户团队收集每个确认的阿里云资源的资产所有者，角色和相关详细信息。
7. 济通科技提供服务中台和工作沟通群为所有阿里云相关查询/问题升级的联系接口。

2.2 托管运维服务项目

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。济通科技为客户提供监控平台的登录权限，可以通过监控平台实施查看用户系统的监控信息。包含：

   - 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 或 catalina.bat 中添加 jmx 配置并重启服务）；

     *Nginx（需在 nginx.conf 中添加 server 并重启服务）；

     *MySQL（需要创建执行 status、extended-status 权限的用户）；

     *MongoDB（需要创建执行 db.serverStatus()权限的用户）；

     *Redis（需要创建执行 info 权限的权限）；

     *ZooKeeper（需要获取 zk 的监听地址及端口）；

     *php-fpm（需在 php-fpm.conf 中开启 pm.status_path，在 Nginx 中添加 location 并重启服务）；
   - 端口监控（无限制）；
   - 5 个 URL 监控（每个 URL 提供 3 个监测点）；
   - 云产品（ECS、RDS、SLB、OSS 等）的性能和过期时间监控（需要只读权限的 AK 信息）。
   - 其他自定义监控

例：监控模板如下：

济通科技监控模板内容					
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：	*8080，8088，9090，8090*				
URL 监控：					
监控内容：	□ https	■ http	■ api		
URL：	api 接口、官网				

例：监控报警的规则如下：

应用产品	报警名称	报警触发规则
ECS	CPU 使用率（CPUUtilization）	每分钟检测一次，连续三次>=90%
	磁盘使用率（vm.DiskUtilization）	每分钟检测一次，连续三次>=90%
	内存使用率（vm.MemoryUtilization）	每分钟检测一次，连续三次>=90%
	等待 IO 操作的 CPU 百分比（cpu.iowait）	每分钟检测一次，连续三次>=60%
	inode 使用率（fs.inode）	每分钟检测一次，连续三次>=90%
RDS	连接数使用率	每五分钟检测一次，连续一次>=80%
	只读实例延迟	每五分钟检测一次，连续一次>=5
	IOPS 使用率	每五分钟检测一次，连续一次>=80%
	CPU 使用率	每五分钟检测一次，连续一次>=80%
	磁盘使用率	每五分钟检测一次，连续一次>=80%
	内存使用率	每五分钟检测一次，连续一次>=90%
SLB	监听每秒丢失连接数（DropConnection ）	每分钟检测一次，连续三次>0
	最大连接数使用率	每分钟检测一次，连续三次>=80%
	QPS 使用率	每分钟检测一次，连续三次>=80%
	后端异常 ECS 实例个数	每分钟检测一次，连续三次>0
云 Redis	CPU 使用率 （CpuUsage）	每分钟检测一次，连续三次>=80%
	连接数使用率（ConnectionUsage）	每分钟检测一次，连续三次>=80%
	内存使用率（MemoryUsage）	每分钟检测一次，连续三次>=80%
	QPS 使用率	每分钟检测一次，连续三次>=80%
云 MongoDB	CPU 使用率	每分钟检测一次，连续三次>=80%
	内存使用率	每分钟检测一次，连续三次>=80%
	磁盘使用率	每分钟检测一次，连续三次>=80%
	IOPS 使用率	每分钟检测一次，连续三次>=80%
	连接数使用率	每分钟检测一次，连续三次>=80%
DRDS	CPU 使用率	每分钟检测一次，连续三次>=80%
	内存使用率	每分钟检测一次，连续三次>=80%
	DRDS 对于每条 SQL 的平均响应时间大于 3 秒	每分钟检测一次，连续三次>=3000
	DRDS 发送到 RDS 的 SQL 的平均响应时间大于 3 秒	每分钟检测一次，连续三次>=3000
CDN	命中率	每分钟检测一次，连续三次<20%
云 Elasticsearch	集群状态异常	每分钟检测一次，连续三次>=2
	节点磁盘使用率	每分钟检测一次，连续三次>=80%
	节点堆内存使用率	每分钟检测一次，连续三次>=80%
	节点 CPU 使用率	每分钟检测一次，连续三次>=80%
	FullGc 次数异常	每分钟检测一次，连续五次>=1
	快照状态失败	每分钟检测一次，连续五次>=2
Linux/Windows	主机内存使用率大于 90% (非 ECS)	每分钟检测一次，连续三次>=90%

	主机可用内存小于 100M	每分钟检测一次，连续三次<100M
	主机 CPU 平均每核负载大于 5	每分钟检测一次，连续三次>5
	主机 CPU 使用率大于 90% (非 ECS)	每分钟检测一次，连续三次>=90%
	主机 CPU iowait 大于 20% (非 ECS)	每分钟检测一次，连续三次>=20%
	主机刚才发生重启	每分钟检测一次，连续三次<0
	主机文件系统剩余空间小于 5%并且小于 5G (非 ECS)	每分钟检测一次，连续三次<5% & <5G
	主机文件系统剩余空间小于 10%并且小于 10G (非 ECS)	每分钟检测一次，连续三次<10% & <10G
	主机文件系统剩余 inode 小于 5% (非 ECS)	每分钟检测一次，连续三次<5%
Processes	进程没有正常运行	每分钟检测一次，连续三次!=1
Ping	地址 Ping 不通	每分钟检测一次，连续三次!=0
Website	站点返回失败	每分钟检测一次，连续三次!=0
Port	端口没有正常运行	每分钟检测一次，连续三次!=0
Apache	Apache 占用 CPU 负载大于 80%	每分钟检测一次，连续三次>=80%
	Apache 刚刚发生重启	每分钟检测一次，连续三次<0
Nginx	Nginx 刚刚发生重启	每分钟检测一次，连续三次<0
PHP	PHP 有处于等待的进程	每分钟检测一次，连续三次>0
	PHP 启用最大进程数受限	每分钟检测一次，连续三次>0
Java	Java 占用 CPU 负载大于 80%	每分钟检测一次，连续三次>=80%
	Java 非堆内存使用率大于 80%	每分钟检测一次，连续三次>=80%
	Java 堆内存使用率大于 80%	每分钟检测一次，连续三次>=80%
	Java 刚刚发生重启	每分钟检测一次，连续三次<0
Tomcat	Tomcat 占用 CPU 负载大于 80%	每分钟检测一次，连续三次>=80%
	Tomcat 非堆内存使用率大于 80%	每分钟检测一次，连续三次>=80%
	Tomcat 堆内存使用率大于 80%	每分钟检测一次，连续三次>=80%
	Tomcat 刚刚发生重启	每分钟检测一次，连续三次<0
MySQL	MySQL 主从延迟过大	每分钟检测一次，连续三次>=0
	MySQL 主从同步线程异常	每分钟检测一次，连续三次=0
IIS	IIS 刚刚发生重启	每分钟检测一次，连续三次<0
	IIS 未设置开机启动	每分钟检测一次，连续三次!=2
	IIS 没有正常运行	每分钟检测一次，连续三次!=4
Docker	Docker CPU 使用率大于 90%	每分钟检测一次，连续三次>=90%
	Docker 内存使用率大于 90%	每分钟检测一次，连续三次>=90%
Zookeeper	Zookeeper 平均响应时间大于 3 秒	每分钟检测一次，连续三次>3

	Zookeeper 等待请求数大于 10	每分钟检测一次，连续三次>10
	Zookeeper 打开的文件描述符使用率大于 80%	每分钟检测一次，连续三次>=80%
RabbitMQ	RabbitMQ 剩余磁盘空间已小于最小限制	每分钟检测一次，连续三次<0
	RabbitMQ 打开的文件描述符使用率大于 80%	每分钟检测一次，连续三次>=80%
	RabbitMQ 内存使用已超出限制	每分钟检测一次，连续三次<0
	RabbitMQ Erlang 进程使用率大于 80%	每分钟检测一次，连续三次>=80%
	RabbitMQ Socket 使用率大于 80%	每分钟检测一次，连续三次>=80%
	RabbitMQ 健康状态异常	每分钟检测一次，连续三次!=0
Kafka	Kafka 失效副本分区大于 0	每分钟检测一次，连续三次>0
	Kafka 队列请求时间大于 3 秒	每分钟检测一次，连续三次>3
	Kafka 队列响应时间大于 3 秒	每分钟检测一次，连续三次>3
Elasticsearch	Elasticsearch 集群状态为 yellow	每分钟检测一次，连续三次=2
	Elasticsearch 集群状态为 red	每分钟检测一次，连续三次=3
	Elasticsearch 打开文件描述符使用率大于 80%	每分钟检测一次，连续三次>=80%
	Elasticsearch CPU 使用率大于 80%	每分钟检测一次，连续三次>=80%
	Elasticsearch 堆内存使用率大于 80%	每分钟检测一次，连续三次>=80%
Kubernetes	Kubernetes deployment 不可用	每分钟检测一次，连续三次>0
	Kubernetes node 不可调度	每分钟检测一次，连续三次>0
	Kubernetes pod 处于失败状态	每分钟检测一次，连续三次>0
	Kubernetes container 已被终止	每分钟检测一次，连续三次>0
	Kubernetes 活跃的 pods 数小于 70%	每分钟检测一次，连续三次<70%

1) 系统监控内容包含：

- 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

requestCount	请求次数
errorCount	错误次数
processingTime	每秒响应处理时间
bytesSent	发送流量
bytesReceived	接收流量
maxThreads	最大线程数
currentThreadCount	当前线程数
currentThreadsBusy	当前繁忙线程数
hitCount	目录缓存命中率
lookupCount	目录查找次数
ProcessCpuLoad	实例 cpu 利用率
SystemCpuLoad	系统 CPU 利用率
SystemLoadAverage	系统平均负载
Uptime	启动时间
serverInfo	版本
SpecVersion	jdk 版本
HeapMemoryUsage	堆内存使用率
2.Nginx 监控项	
监控内容	监控内容解释
active	活跃的连接数量
accepts	总共处理的连接数
handled	成功创建的握手次数
requests	总共处理的请求数
reading	读取客户端的连接数
writing	响应数据到客户端的数量
waiting	已经处理完正在等候下一次请求指令的驻留连接

3.Zookeeper 监控项	
监控内容	监控内容解释
approximate_data_size	近似数据总和大小
avg_latency	平均响应延迟
ephemerals_count	临时节点数
max_file_descriptor_count	打开文件描述符数
max_latency	最大响应延迟
min_latency	最小响应延迟
num_alive_connections	活跃连接数
open_file_descriptor_count	打开文件数量
outstanding_requests	排队请求数
packets_received	接收数据包
packets_sent	发送数据包
version	版本信息
watch_count	watch 数
znode_count	znode 数
followers	集群 follower 的个数
synced_followers	已同步的 Follower 数
pending_syncs	阻塞中的 sync 操作

4. Redis 监控项	
监控内容	监控内容解释
active_defrag_hits	主动碎片整理命中次数
active_defrag_key_hits	主动碎片整理 key 命中次数
active_defrag_key_misses	主动碎片整理 key 未命中次数
active_defrag_misses	主动碎片整理未命中次数
bigkeys_status	大 key 状态

blocked_clients	正在等待阻塞命令的客户端的数量
client_biggest_input_buf	当前连接的客户端中最大输入缓存
client_longest_output_list	当前连接的客户端中最长的输出列表
clients	连接的客户端数量

2) 阿里云资源监控内容包含：

- 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 RDMP 服务中台，并反馈通知到运维群及运维人员（钉钉或企业微信群）。
- 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 RDMP 服务中台通知到运维群及运维人员。
- 云资源相关升级/变更监控。

例：阿里云资源监控如下：

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

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 5 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）。

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，济通科技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。

4) 系统异常处理内容包含

- 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。

5) 应用异常处理

根据监控结果对应用的异常做应急响应与异常处理。

6) 阿里云资源相关异常处理

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

3. 日常运维服务

包含环境设置、安装部署、中间件参数调配、数据备份、升级/变更资源等操作。

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

例：阿里云资源运维事项

Service Module	Items	Details-EN	Details-CN
Computing	VM management	Create ECS	创建 ECS
		Delete ECS	删除 ECS
		Change ECS State：start|stop|restart	ECS 状态变更：start|stop|restart
		ECS info & Status Check	ECS 信息和状态查看
		ECS Up-scale or salce down	ECS 扩容和降配
	OS	OS Setup	操作系统安装
		OS Initialization	操作系统初始化设置
		Password Initilization	密码初始化
		New-added Disk，Partition，Attached	新增磁盘，磁盘分区和挂载

		Scale up Disk Space	磁盘空间的扩容
		Analyze System Log	分析系统日志
		troubleshooting	故障排查
	Storage	Create bucket	存储桶的创建
		Create bucket policy	存储桶策略配置
		Setup read & write permisson of bucket	存储桶读写权限设置
		Setup object permission of bucket	存储桶对象权限设置
		Delete bucket/objects	存储桶或对象删除
		Check bucket/object info & state	存储桶或对象信息或状态查看
		Create, change, attach/unattached volume	磁盘的创建、附加和卸载
	Autoscaling	Autoscaling setup	自动伸缩集群创建
		Autoscaling policy setup & configuration (Policy Management, Schedule, Inistance)	自动伸缩策略及设置（策略管理，周期，实例个数等）
		Autoscaling State Confirmation	自动伸缩集群状态确认
		Alerts (E-Mail, SMS)	告警（邮件，短信）
	Keypair	KeyPair Creation	秘钥对创建
		KeyPair associate to ECS	秘钥对关联 ECS
		Cancel association between KeyPair and ECS	取消秘钥和 ECS 关联
		KeyPair Delete	秘钥对删除
	web server installation	Nginx/Apache Installation	Nginx/Apache 安装
	was server installation	JDK/Tomcat/PHP/weblogic/python	JDK/Tomcat/PHP/weblogic/python
Network	CDN	Config Domain HTTP Acceleration	域名 HTTP 加速设置
		Config Domain HTTPs Acceleration	域名 HTTPS 加速设置
	DNS	DNS record change (add/delete/modify)	DNS 记录变更（添加/删除/修改）
		Import/Export Records	导入导出记录
	LB	Internal/Public Server Load Balancer Creation	内网/公网 LoadBalancer 创建
		Server Load Balancer Config and Testing	负载均衡配置和调试
		Add ECSs after Server Load Balancer	将 ECS 注册到负载均衡
		Remove ECS out of Server Load Balancer	取消 ECS 到负载均衡的注册
		Server Load Balancer Delete	负载均衡删除
	VPC	VPC Network Planning	VPC 网络规划
		VPC Subnet Creation	VPC 子网创建
		VPC ACL Creation	VPC ACL 创建
		VPC ACL Rules Add & Delete	VPC ACL 规则的添加和删除
		Modify VPC Subnet	VPC 子网的调整
		Delete VPC Subnet	VPC 子网的删除
		VPC Creation or Delete	VPC 创建和删除
		VPC Routetable Setup	VPC 路由表的设置
	VPN	VPN Connection Creation	VPN Connection 创建
		VPN Connection Config	VPN Connection 配置
		VPN Connection Delete	VPN Connection 删除

Security	WAF	WAF user management	WAF 用户管理
		WAF permission management	WAF 权限管理
		WAF Rules management	WAF 规则管理
	Network security group	NSG Creation	网络安全组的创建
		NSG Rules New-added, change, delete	安全组 规则的新增、变更和删除
		Delete NSG	网络安全组的删除
	Unplanned patch	Linux Patch Upgrade	Linux 系统补丁更新
		Windows Patch Upgrade	Windows 补丁更新
		DB Patch Upgrade	DB 补丁更新
		Cloud Patch Update	云平台补丁更新
	Cloud user permission management	RAM User/Group Management	RAM 用户/组管理
		Role & Policy Management	角色和策略管理
		MFA Enable/ Disable	MFA 启用和禁用
	OS user permission management	OS User & Keypair	操作系统用户和秘钥对
	DB user permission management	DB User management	DB 账户管理
	SSL Certificates Management	SSL Certification deployment	SSL 证书部署

2) Linux系统运维

- 操作系统安装和配置
- 磁盘配置与管理
- 用户和组管理：用户创建、密码重置、解锁用户、禁用用户
- 开源 Web 中间件（Apache、Tomcat、Nginx 等）的安装、配置等技术支持
- 开源应用中间件（ElasticSearch、ActiveMQ、Zookeeper 等）的安装配置及技术支持
- 第三方商业/付费软件，需要有软件供应商支持和协助的前提下，进行运维支持
- 为开发团队提供各种开发语言的环境部署与支持
- 性能优化，补丁，小版本升级
- 安全修复程序和内核参数，以满足应用程序安装验证和先决条件
- 配合客户运维人员实施备份

3) Windows系统运维

- 操作系统安装和配置
- 磁盘配置与管理

- 活动目录，网络访问、文件和打印服务功能
- 用户和组管理：用户创建、密码重置、解锁用户、禁用用户
- 性能优化，升级 Windows 补丁及更新
- 应用程序安装验证、更新和先决条件
- 开源 Web 中间件（Apache、IIS、Tomcat、Nginx 等）安装、配置及技术支持
- 微软办公套件技术支持
- 第三方商业/付费软件，需要有软件供应商支持和协助的前提下，进行运维支持
- 为开发团队提供各种开发语言的环境部署与支持
- 协助客户运维人员进行防病毒管理
- 配合客户运维人员实施备份

4) 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

5) 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

4. 安全运维服务

提供云平台、操作系统、数据库等安全运维加固，安全事故处理。

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。通过使用济通科技服务团队优化过后的系统镜像替代初始化镜像，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
- 添加用户登陆警告信
- 限制外网登陆 IP,所有远程登录入口均为堡垒机

2) 补丁管理/安全警报

- 基于阿里云安全团队或平台建议，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。
- 济通科技安全服务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，济通科技安全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。

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、SDWAN 咨询服务

1) VPC规划服务

- VPC 网段的规划、创建服务；
- VPC 路由调整服务；

2) VPN部署调试服务

- VPC 环境下的 VPN 配置服务
- 经典网络下的 VPN 配置服务
- 金融云 VPC 环境下的 VPN 配置服务

备注：为客户提供的 VPN 配置服务，仅包括阿里云上的 VPN 安装、配置，涉及到客户线下设备配置由客户配置，济通科技网络团队将会在整个 VPN 调试过程中配合客户完成本次 VPN 的调试。

3) VPN故障排除服务

- 阿里云上 VPN 的日志分析、故障排查
- 阿里云上 VPC 路由的分析
- 协助分析客户侧 VPN 问题

4) 提供专线咨询服务

- 协助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

6. 数据库服务

包括数据库安装、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（**Oralce 数据服务需单独收费，详见数据库服务说明书**）。

- 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 监控和故障响应
- 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) 安装配置服务

- 配合用户在指定的系统上安装数据库软件（涉及到商业版本数据库安装需要客户提供授权）
- 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

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

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

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

5) 性能优化

首先提供数据库的监控，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
- 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：控制台报警由机器人自动发送至钉钉或群者企业微信群并触发告警升级流程
- 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

6) 数据库系统参数调整与优化

- 数据库系统配置优化
- SQL 语句优化，主要通过修改 SQL 的优化查询速度，表索引的合理性
- 硬件架构，提高硬盘的 IO 速度，redo 的磁盘分布等
- 数据库系统参数调整

7) 数据库系统迁移（增值服务）

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

7. 月报/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济通科技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，济通科技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(月报)

- 月总结报告

2) 事件报告（月报）

3) 安全报告(月报)

- 主机安全
- 漏洞

4) WEB报告(月报)

- URL 监控

5) 主机报告 (月报)

- 基础监控
- 端口监控

6) 数据库报告(月报)

服务水平协议SLA

责任和假设
云托管运维服务

1. 服务水平协议SLA

济通科技在托管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，并向客户指定的运维服务团队报告。 问题分为以下四个类别，响应时间定义如下表 1 所示。

以下政策仅适用于济通科技 Cloud Maintenance 的“云托管运维服务”。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

客户也可以通过 RDMP 服务中台或钉钉群提交事件（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济通科技重点审查的任何系统操作故障或异常情况。事件必须使用济通科技提供的 RDMP 服务中台或钉钉群进行提交，紧急情况下可先通过电话沟通。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：Cloud Maintenance 的事件仍以 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。	15 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。	15 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，RDMP 服务中台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。 Cloud Maintenance 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. 阿里云托管条款

Cloud Maintenance 会监控阿里云托管服务的 SLA。服务等级积分将根据阿里云设置的政策进行定义和退款，

并且不加标记地提供给客户。 请参阅以下链接了解更多详情:

ECS SLA:

http://terms.aliyun.com/legal-agreement/terms/suit_bu1_ali_cloud/suit_bu1_ali_cloud201802111644_54047.html?spm=a2c4g.11186623.2.7.24d721591M6VaT

RDS SLA ：

http://terms.aliyun.com/legal-agreement/terms/suit_bu1_ali_cloud/suit_bu1_ali_cloud201803061219_30806.html?spm=a2c4g.11186623.2.47.5c981408VNUNCr

其他产品的 SLA 通过

https://help.aliyun.com/document_detail/56773.html?spm=a2c4g.11186623.2.10.fe19252ayro2Ka#title-cc0-k3n-own

搜索

3. 客户责任

为了圆满地完成本工作说明书所定义的工作，Cloud Maintenance MSP 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项目经理以及第二项目经理（备用），负责协调所有与客户有关的活动，并作为与济通科技沟通的联络接口人，根据需要协助双方之间的问题。当第一项目经理不在时，第二项目经理将作为联络接口人。 项目经理将:
    a. 作为客户内部部门和济通科技团队之间的接口;
    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. Cloud Maintenance 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，在使用 RDMP 服务中台产品和服务时在该机器上安装 RDMP 相关组件(包含堡垒机及监控平台)，该机器配置为 4c8g 且可访问公网。
3. 客户应提供必要的网络能让济通科技服务团队远程访问以提供技术服务。
4. 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。
5. 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。

6. 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。
7. 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）。

4. 假设

为了支撑本服务内容，济通科技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. 济通科技服务工程师将利用 RDMP 服务中台来记录和跟踪问题，双方都将有权使用此工具。
3. 设定通用的电子邮件 ID（例如，service@trisfal.com）。 所有的电子请求都会发送到这个电子邮件 ID。
4. 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。
5. 客户有云下服务器托管运维要求时，须满足以下先决条件；
   - 所有的服务基于远程方式，客户应保证远程访问线下机房服务器资源的网络可达。
   - 客户应负责服务器上下架、服务器宕机维护重启、存储介质更换等硬件层面的运维，我司提供操作系统及以上层面的运维。

数据所有权和访问权限转移策略

数据所有权和访问权转让策略旨在规定协议终止的情况下确保妥善处理数据的条件和准则（或由于任何济通科技行为或不作为导致的阿里云客户许可条款中止），以及这种处理的选项是明确定义和执行的。

配置的阿里云基础设施上存储的数据作为本次交易中一部分其所有权，头衔和利益应归属客户。 在本协议终止的情况下，客户自行决定使用以下方法之一处理客户数据：

a) 如果客户希望继续使用阿里云，那么阿里云账户的所有权（包括财务责任）将转移到由客户以书面形式正式确定的客户联系人。账户所有权的转移包括但不限于：
   - 禁用与济通科技管理员或工具关联的所有 RAM 登录
   - 共享阿里云帐户根凭证和正在使用的任何密钥对
   - 提供必要的帮助来配置阿里云付款方式（信用卡/发票）
b) 如果客户选择不继续进行阿里云托管，并希望将数据传输到其网络，济通科技将通过 IPSEC 隧道/直接连接或使用阿里云导出/导入服务来进行数据传输。
c) 根据客户要求，济通科技将根据阿里云推荐的方法，删除/终止客户书面规定的阿里云帐户中的所有资源。
d) 济通科技将遵循客户书面规定的并符合阿里云安全最佳实践部分定义的安全要求的任何其他可选途径。

与客户项目经理协商确定适当的数据处理方法。书面授权将被要求确认启动所有权和访问的转移。 在完成转移过程后，客户需要书面接受确认和结束。 所有阿里云存储资源（包括那些可能包含关键数据的资源）将保留不超过转移后十个日历日的时间，以便有足够的时间让客户确认数据的一致性和完整性。 转移十天后，所有阿里云资源将被彻底删除，不可恢复。 在上述所有情况下，济通科技在所有权和访问转移期间产生的使用费用将以成本价格转交给客户，而不会对阿里云费率进行任何额外的加价。

附件一 《云托管运维服务规范》

1 安全规范

甲方给到乙方代维的对应服务器，需要严格遵守乙方相关安全加固规范。如若不按照此安全规范而产生的对应运维安全事故，相应责任需由甲方承担。

乙方提供的安全监控平台是基于堡垒机的安全运管平台。甲方和乙方所有人员对运维资源的管理都以RDMP 服务中台为入口，操作记录全部被记录下来，便于审计和记录。目前堡垒机的主要功能包含：

1)用户管理组件

用户管理组件包括用户的新增、修改、删除、查看、重置密码等功能。用户必须隶属于该公司。用户可以绑定邮箱用于开通、重置密码等功能。用户分为普通用户以及管理员,管理员可以使用所有资源并给普通用户分配可以管理的资源组,普通用户只能由管理员分配。

2)资源组管理组件

资源组管理组件包括资源组的新增、修改、删除、查看等功能。资源组分为普通资源组以及网络默认资源组,管理员可以创建资源组,管理员以及资源组管理员可以对资源组进行资源添加/删除操作。

3)资源管理组件

资源管理组件包括资源的添加、修改、删除、查看等功能,资源分为服务器管理、数据库管理和负载均衡,服务器支持 Windows 以及 Linux,数据库支持主流数据库，负载均衡支持主流云厂商的产品。

4)日志管理组件

日志管理组件包括日志的收集、查看以及搜索等功能。用户通过管控节点操作服务器或者数据库的所有输入以及输出(数据库不包含输出)都会被记录下来并且上报给堡垒机,用户可以在堡垒机上按时间顺序查看搜索日志,以达到安全审计的要求。

5)连接管理组件

连接管理组件包括在线连接(包括网页 SSH,通过 SSH 隧道连接,RDP 以及通过 MySQL 隧道连接)的查看、监控以及强制断开等功能。管理员或者资源组管理员可以实时监控在线连 接,看到用户的所有操作,也可以强制断开一个连接。

6)管控节点组件

a. SSH 隧道，用户可以利用管控节点的 SSH 隧道功能通过管控节点连接目标服务器的 SSH 服务,与正常使用 SSH 登录目标服务器的方式相同。

b.RDP 工具，用户可以通过 RDP 客户端连接目标服务器的 RDP 服务进行操作,所有的操作将会被录屏并支持回放。

2.账号规范

2.1 运维账号

乙方统一采用 trops 用户登录服务器进行运维操作，具备 sudo 权限。

甲方统一采用 xxadmin 用户登录服务器进行日常操作，具备 sudo 权限；采用 www 用户启动应用程序，不需要有 root 权限。

乙方需为甲方提供 RDMP 服务中台的账号和权限。

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进行运维工作，该账号需要甲方赋予管理所有阿里云资源的权限的权限（AdministratorAccess）。

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，方便乙方为甲方收集月报信息、监控阿里云云产品等场景中使用。

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.服务对接规范

1. 甲方需为本运维服务合同指定一名主要联系责任人以及至少一名次要联系人。联系人要加入到甲方 RDMP 企业账号中，联系方式包括电话和邮箱。

2. 乙方需为甲方指定项目负责人、运维人员等联系人。运维服务合同服务内容的对接需由双方责任人承担，双方需遵守此服务规范。如若单方不遵守此规范，所带来问题责任需由单方承担。如甲方没有通过 RDMP 服务中台或钉钉群提交线上重大变更请求的事件，如乙方非负责人直接处理甲方服务请求等。

3. 甲方以在 RDMP 服务中台发起事件的标准方式提交服务请求，乙方工程师接收事件并审核通过后，可处理甲方服务请求。

4. 若甲方人员服务请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。

5. 关于代码发布，乙方可以协助甲方进行业务代码平台（svn/git）的搭建、自动化工具/平台的搭建，协助甲方规范及简化业务代码的更新发布。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。

4.监控事件服务流程

乙方在甲方系统异常的时候，需以 TR Monitor 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 TR Monitor 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。

乙方 7*24 紧急联系方式如下

紧急联系人：济通科技监控中心

紧急联系电话：0571-56337786

紧急邮箱： service@trisfal.com

5.变更规范

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 RDMP 服务中台或钉钉群发起事件，乙方根据事件内容对资源进行安全加固、监控部署等操作。

5.2 配置变更

甲方有配置变更需求，需要在 RDMP 服务中台或钉钉群发起事件以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。

6.月报规范

乙方需在每月十号前为甲方提供上个月的月总结报告并以邮件方式通知到甲方，月报包含概览、事件报告、安全报告、web 报告、主机报告、数据库报告共 6 部分。

7.事故报告规范

业务系统中断或非正常运行超过 30 分钟等情况下，乙方需为甲方出具事故报告，事故报告包含故障描述、系统及数据库信息、故障分析及处理思路、处理过程、优化建议共 5 部分。