斑羚在线

云上急诊专家服务手册

版本	V1.2
修改日期	2020 年 12 月
编撰人	程棣 牛萍萍

目录

一　服务内容概述

由北京斑羚在线网络科技有限公司（以下简称“斑羚在线”）在云市场上提供的“云上急诊专家”服务，致力于为各行业用户解决上云中遇到的各种难题，尤其是用户员工无法通过即有常识做出正确判断的情况下，斑羚在线将利用自己丰富的行业经验，为用户提供从发现问题、判断性质到如何有效处理问题的一站式解决方案。

二　具体服务内容

1　问题判断

考虑到该用户面对的受众主要是遇到上云中的疑难杂症，且不便自行解决的用户，为更高效地协助用户处理问题，首要重心就是协助用户厘清线索，在暴露出的问题与现象中抽丝剥茧，找到核心根源。为保证该服务实施的有效性，斑羚在线会向用户了解所有可能衍生问题的情况，包括不限于云产品规格、操作系统、主要软硬件等，并在经过用户授权情况下，调查以下监控内容：

监控内容模板					
基础监控：	CPU	Memory	Network	Disk	OS
其他：	客户指定的其他内容				
应用监控：	IIS	Apache	Nginx	Tomcat	Resin
	MyQSL	MSSQL	Oracle	MangoDB	Redis
	Memcached	RDS-MySQL	RDS-MSSQL	KVStore	Zookeeper
其他：	客户指定的其他内容				
端口监控：	80	22	3306	1433	21
其他：	443、8080、8088、6379 等				
URL 监控：					
API 接口：					
其他自定义：	如 error 日志报警				

监控报警规则（需用户授权）：

No	大类	分类	监控间隔（分）	Alert 邮件发送机制
1	OS 运行	zy_agentping	1	异常时，每 1 分钟 check 一次，5 次后仍异常则发信
2	性能监控（OS 系）	CPU 使用率（%）	1	
		CPURunQueue（LordAverage）	1	
		空 Memory 率（%）	1	
		空 Swap 域	无	可根据需求自主设定
3	Disk 使用率（OS 系）		1	异常时，每 1 分钟 check 一次，3 次之后仍异常则发信
	DiskIO（OS 系）	磁盘读写	1	每 1 分钟 check 一次，3 次之后仍异常则发信
	进程数（OS 系）	主机运行的进程数	1	每 1 分钟 check 一次，3 次之后仍异常则发信
4	Process（OS 系）		1	每 1 分钟 check 一次，3 次之后仍异常则发信
5	Port		1	每 1 分钟 check 一次，3 次之后仍异常则发信
6	Log		1	主动监控关键字，出现关键字则发信
7	URL		2	监控反馈状态，当返回值不为 200 时则发信
8	RDS	CPUUtilization	5	每 5 分钟 check 一次，一发现异常即发信
		DatabaseConnections	5	每 5 分钟 check 一次，一发现异常即发信
		IOPS	5	每 5 分钟 check 一次，一发现异常即发信
9	文件删改		1	一发现异常即发信

- 系统监控内容包括：

✓ 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、运行进程数等；

✓ CPU、磁盘、内存、网卡等系统性能状态监控，包括：CPU 使用率、CPULord、内存使用臃、网络出入网流量、磁盘使用空间、磁盘 IO 等；

✓ 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；

Tomcat 监控项目	
监控内容	解释
Tomcat version	Tomcat 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
Tomcate-http-80-活动线程	Tomcat 使用的线程数据
Tomcate-http-80-线程峰值	Tomcat 使用的最大线程数
Tomcate-http-80-线程总计	Tomcat 线程数问题
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
Nginx 监控项	
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
Zookeeper 监控项	
监控内容	解释
zk_avg_latency	
zk_ephemerals_count	
zk_followers	
zk_max_file_descriptor_count	
zk_max_latency	
zk_min_latency	
zk_num_alive_connections	

zk_open_file_descriptor_count	
zk_outstanding_requests	
zk_pactets_received	
zk_packets_sent	
zk_running_ok	
zk_server_state	
zk_synced_followers	
zk_version	
zk_watch_count	
zk_znode_count	

Redis 监控项	
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

✓ 通过脚本扩展的自定义监控项状态监控

- 服务器资源监控内容包括：

✓ 服务器资源 ECS/SLB/RDS/OSS 乃朋友其他云服务等相关监控。通过调用服务器相应资源的 API，获取监控和报警数据，并将情况反馈给客户；

✓ 资源过期监控预警：对于资源过期的 API 资源，例如 ECS 等产品，通过 API 调取资源过期时间，在资源到期之前反馈客户；

✓ 云资源相关升级/变更监控

RDS for MyQSL 监控项	
监控内容	解释
MyQSL_COMDML_com_delete	平均每秒 Delete 语句执行次数
MyQSL_COMDML_com_insert	平均每秒 Insert 语句执行次数
MyQSL_COMDML_com_insert_select	平均每秒 Insert_Select 语句执行次数
MyQSL_COMDML_com_replace	平均每秒 Replace 语句执行次数
MyQSL_COMDML_com_replace_select	平均每秒 Replace_Select 语句执行次数
MyQSL_COMDML_com_select	平均每秒 Select 语句执行次数
MyQSL_COMDML_com_update	平均每秒 Update 语句执行次数
MyQSL_InnoDBBufferRatio_ibuf_dirty_ratio	缓冲池脏块的百分率

MyQSL_InnoDBBufferRatio_ibuf_read_hit	缓冲池的读命中率
MyQSL_InnoDBBufferRatio_ibuf_use_ratio	缓冲池的利用率
MyQSL_InnoDBDateReadWriten_inno_date_read	平均每秒读取的数据量
MyQSL_InnoDBDateReadWriten_inno_date_written	平均每秒写入的数据量
MyQSL_InnoDBLogWrites_Innodb_log_writes	平均每秒向日志文件的物理写次数
MyQSL_InnoDBLogWrites_Innodb_log_write_requests	平均每秒日志写请求数
MyQSL_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 平均每秒从硬盘上读取的次数
MySQL_MyISAMKeyReadWrites_myisam_keyr_r	MyISAM 平均每秒从缓冲池中的读取次数
MySQL_MyISAMKeyReadWrites_myisam_keyr_w	MyISAM 平均每秒从缓冲池中的写入次数
MySQL_MyISAMKeyReadWrites_myisam_keyw	MyISAM 平均每秒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
MyQSL_RowDML_Inno_log_writes	平均每秒向日志文件的物理写次数
MyQSL_RowDML_Inno_row_delete	平均每秒从 InnoDB 表删除的行数
MyQSL_RowDML_Inno_row_insert	平均每秒从 InnoDB 表插入的行数
MyQSL_RowDML_Inno_row_readed	平均每秒从 InnoDB 表读取的行数
MyQSL_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

- 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)。

✓ 网站首页或其他应用地址监控（默认首页)；

✓ API 接口监控（需用户提供 API 接口)；

✓ 模拟用户登录、查询等应用监控（需用户提供 API 接口）。

2 常规问题处理

经过先期沟通与问题查找环节，斑羚在线会根据专业判断向用户提供最精准可行的解决方案，并进行职能划分建议，如涉及不便对外公开的业务流程与细节，斑羚在线可在用户自行处理时进行场外协助；如用户授权斑羚在线专家人员予以处理，根据具体情况，用户需提供阿里云后台、服务器、数据库及所涉业务的帐号密码以便操作。

专家服务处理内容，包括系统异常处理、应用异常处理、服务器资源异常处理。如发现异常是由于客户程序或不当操作导致，专家也会及时通知客户进行改进。

- 系统异常处理内容包括：

✓ 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监控项状态异常处理。

- 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。

- 服务器资源异常处理

✓ 宕机迁移、RDS 异常及其他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事故处理。

3 安全问题处理

如经过前期调查，确定用户问题为受到网络攻击所至，斑羚在线将为用户提供系统安全运维加固、应用安全扫描、安全事故处理来解决出现的问题。

- 运维安全加固

针对不同应用，进行系统层、应用层、网络层安全加固，通过优化系统镜像替代原始镜像，对安全组和主机对外端口进行安全设置。

- 系统安全扫描

针对服务器，进行系统层安全渗透扫描，给出基础的安全报告。

- 应用安全扫描

针对用户业务，进行应用层安全渗透扫描，给出基础的安全报告。

4 问题反馈

问题解决后，斑羚在线会将问题原因、解决建议、处理流程及其他优化建议以文档形式定期提供给用户。

- 报告内容

可能含有基础运维数据统计、安全数据统计分析、系统构架优化建议、采购优化建议、软件优化建议，业务故障分析及改进建议等，并根据实际情况予以补充。

- 报告特色

✓ 各类型数据详实，来源可溯，云资源数据来自官方控制台，经用户授权（主要以 RAM 形式为主）获取，其他数据来源通过用户开放 API 端口或其他系统端口获取；

✓ 站在用户角度，对事件及故障内容进行详细的客观描述，包括影响范围、时长，事件发

生的原因（或可能性）、事件处理的过程和结果，如需要额外采购产品来解决现有问题，还将包含后续处理的计划和预算等安排，待用户审核确认。

三 服务流程及服务等级协议

1 安全规范

甲方要求乙方进行代运维的服务器，需严格遵守乙方安全加固规范，如未按照此安全规范操作产生的运维安全事故，需由甲方承担相应责任；同时，乙方同样需要按照规程及安全措施进行操作，未经甲方授权及同意，不得单方面进行任何涉及应用层的操作，如因此造成甲方损失，将由乙方承担相应责任。

2 服务对接

- ✓ 甲方需为运维服务指定一名主要负责人及至少一名次要联系人。联系方式包括：电话、邮件地址、IM 工具（钉钉、微信）。乙方需为同一项目指定项目负责人及具体运维工程师一名。运维服务内容对接由双方责任人共同承担，如某一方未遵守此规范，所产生问题责任由该全权承担。
- ✓ 为保障工作效率，甲方日常咨询可通过 IM 工具即时与乙方沟通，如涉及正式服务请求，需以官方邮件方式进行确认。
- ✓ 如甲方提出需求有可能影响业务运转或威胁系统安全，乙方需向甲方提出警示，如甲方确认照此执行，则乙方在收到甲方主要联系人需出具的书面确认函（加盖公章）后执行，以明确双方经济与法律责任。

- ✓ 乙方可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，并协助甲方规范及简化业务代码，但不负责甲方业务代码层的更新发布、异常解决、bug 修复等。

3 监控事件服务流程

乙方在监控到甲方系统异常时，需以电话/邮件方式 7*24 小时通知到对方。乙方默认提供服务时间为 5*8 小时，但当甲方出现核心业务异常，无法正常访问、服务器宕机等级别事件时，乙方将临时将服务提升至 7*24 小时级别。

4 运维需求服务流程

斑羚在线运维需要分为四个级别，应对的响应时间和处理周期请见下表：

故障级别	故障级别描述	响应时间	处理周期
一级	紧急问题，其具体表现包括：系统崩溃导致业务中断、数据丢失（非业务代码问题）	立即	1 小时
二级	严重问题，其具体表现包括：出现部分功能失效、业务可运行，但系统性能下降，如高负载、流量短期内过高等	立即	2 小时
三级	较严重问题，其具体表现包括：系统报错或警告、软件日志报错或警告、程序日志报告或警告，但业务系统能持续运行且未影响性能	立即	4 小时
四级	普通问题，其具体表现包括：系统技术功能、安装或配置咨询，或其他明显不影响业务的预约服务	立即	8 小时

四 服务变更流程

在项目实施过程中，任意一方意图更改双方事先确认好的服务内容，包括但不限于运维服务器、数据库资源增减等，均须向对方提交《项目变更请求表》，表中包含实施范围更改、实施周期更改、实施方案变更等内容。双方针对变更内容重新估算项目进度、附加费用、交付效果，并经双方领导审批通过后予以执行。

1 提出变更

提出方以书面文件形式将《项目变更请求表》向对方呈递；

2 接收方响应

收到文件后，先通过正式邮件告知请求表已收到，并告知对方大致评估时间；

3 双方认可

如涉及额外产生费用，经双方领导共同确认后，将《项目变更请求表》作为附加协议加入原合同文本中，同时替代前期内容相冲突的协议；

4 变更实施

双方根据确认批准的《项目变更请求表》重新进行任务分配，并履行各自责任义务。