ICS 13.310
CCS A 91

WHAF

武 汉 市 安 全 技 术 防 范 行 业 协 会

T/WHAF 002—2020

基于云计算的公共安全视频监控平台服务规范

Cloud computing service specification of public security video monitoring platform

2020-12-30 发布

2021-02-28 实施

武汉市安全技术防范行业协会发布

目　　次

前　言

本文件按照GB/T 1.1—2020给出的规则起草。

本文件由武汉市安全技术防范行业协会提出并归口。

本文件起草单位：武汉迈异信息科技有限公司，景网技术有限公司，湖北省电子信息产品质量监督检验院，湖北省标准化与质量研究院。

本文件主要起草人：刘克华、宋凯、唐湘丕、甘虎标、安维亮、李武、余卫东、晏亮、余毅、王彪、陈琛、张猛、周子新、丁军祥。

核心评审专家：陈国瑞、崔一兵、余莉琪、姚东明、罗学斌、徐煦、牛慎刚。

本文件实施应用中的疑问，可咨询武汉市安全技术防范行业协会，办公地址：武汉市武昌区积玉桥前进路四清村 51 号，联系电话：027-88062600，E-mail：250020733@qq.com。

引　　言

公共安全视频监控体系建设正处于转变发展方式、深化应用和突出成效的转型期。积极探索云计算在公共安全视频监控体系中的应用，充分发挥云计算的虚拟化及高可靠性、通用性、高可扩展性等特点，建立基于云计算的公共安全视频监控平台，将有效实现平台建设的集约化，应用的平台化。只有通过标准化、规范化的服务才能实现对业务和运维的全面支持，提高云计算平台的技术服务能力，为用户提供优质的服务，切实让用户体会到统一管理、统一运维带来的优越性，提高资源利用率。

从业单位在遵循现行湖北省、武汉市行政主管部门要求，符合国家现行保密法律、法规的前提下，依照本文件开展标准化活动，建立完善的云平台服务体系，改变传统的服务方式，会有效整合服务资源，优化服务产品，完善服务制度，提高服务质量，满足用户的需要。

基于云计算的公共安全视频监控平台服务规范

1 范围

本文件规定了基于云计算的公共安全视频监控平台服务的术语和定义、云平台运维要求、云平台安全、费用核准方法。

本文件适用于武汉市基于云计算的公共安全视频监控平台服务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 32400——2015信息技术云计算概览和词汇

GB/T 36326——2018 信息技术云计算云服务运营通用要求

GB/T 35279-2017　信息技术安全云计算安全参考架构

T/WHAF 001-2019　公共安全防范视频监控系统运维服务规范

3 术语和定义

GB/T 32400-2015、GB/T 51399-2019、GB/T 37740-2019 、T/WHAF 001-2019界定的以及下列术语和定义适用于本文件。

3.1

基于云计算的公共安全视频监控平台 public security video monitoring platform based on Cloud Computing

运用云计算技术，统筹利用机房资源、计算资源、存储资源、网络资源、信息资源等，发挥云计算虚拟化、高可靠性、通用性、高可扩展性以及快速、按需、弹性的服务等特征，利用视频技术探测、监视监控区域并实时显示、记录现场视频图像的电子系统，以下简称“云平台”。

3.2

软件原厂技术支持服务　software factory technical support service

云计算平台提供方针对公共安全视频监控云平台运营维护提供的原厂技术支持服务。

3.3

资源池　resource pool

一组物理资源或一组虚拟资源的集合，可以从池中获取资源，也可将资源回收到池中。资源包括物理机、虚拟机、虚拟网络设备、物理网络设备和IP地址等。

3.4

自动巡检　automatic inspection

利用云平台自动化运维工具、自动化运维脚本、物理设备传感器等，持续收集系统、应用、运行环境、设备状态、安全环境等信息，投送至运维看板或运维指挥中心大屏服务，便于用户迅速、及时发现运营维护过程中紧急状态。

3.5

应急响应组织　emergency response organization

视频监控云平台运行维护服务的服务提供方、原厂技术支持方等，在运行维护服务组织基础上建立应急响应组织，以面对视频监控云平台紧急故障情况下的快速响应和恢复工作。

3.6

应急响应制度　emergency response system

包含应急响应的目标、原则、范围以及各项管理要求的制度。

3.7

应急响应预案　emergency response plan

可以分为总体预案和针对单独核心系统的专项预案，应急响应预案的格式能够为应急响应组织进行系统恢复操作提供快速明确的指导。

3.8

运维知识库　operations the knowledge base

运维知识库是运维专家系统设计所应用的规则集合，具有咨询性质，是提升云平台运维能力重要手段，运维方要积极参与运维知识库建设，同时，云平台拥有方应参与监督运维知识库建设。

4　云平台运维要求

4.1　基本要求

4.1.1　建设\使用单位

4.1.1.1　建立规范工作考核机制、管理机制，制定公共安全防范视频监控云计算平台系统使用、运维运营等规章制度，组织落实各项保障措施，确保云平台稳定运行。

4.1.1.2　建立云平台运维运营经费管理制度，列支公共安全防范视频监控云计算平台运营维护服务各专项经费预算，专项经费应做到专款专用，有据可依。

4.1.1.3　云平台运维运营服务工作技术资料应包括以下基本内容：

a) 工程竣工文件包括云平台设计方案、服务器等物理硬件参数清单、产品质量合格证明、产

品/系统使用说明书、施工记录、系统验收报告等；

b) 工程竣工图纸包括系统原理图、网络拓扑图、前端设备布防图、管线敷设图、数据中心布局、接线图等；

c) 系统运行及维保记录包括系统运行情况记录、系统巡检记录、系统改造说明或记录、维护保养记录、故障处置记录等。

4.1.2 运维服务单位

4.1.2.1 应在中华人民共和国境内注册、具有独立法人资格的单位。

4.1.2.2 应具有同类、同规模项目的设计施工和运维服务经历，并具备协助建设/使用单位建立、完善系统运行应急预案的能力。

4.1.2.3 应组建专门的运维服务机构，配备相应的专业运维服务人员。

4.1.2.4 运维服务人员应符合以下条件：

a) 对于从事公共安全防范视频监控云计算平台运维服务工作的人员，运维单位应坚持“先审查、后录用”的原则，并登记备案；

b) 运维服务人员应当接受有关法律知识、安全法规和标准的培训、考核，并遵守相关的保密规定；

c) 运维服务人员应具备与其职责相应的综合素质和业务技能。

4.1.2.5 应配备与公共安全防范视频监控云计算平台运维服务工作相适应的软件工具、设备等。

4.1.2.6 应与建设/使用单位签订保密协议，落实责任与措施。

4.1.2.7 应根据云平台运行情况及安全保卫工作需要，向建设/使用单位提出关于系统/设备升级、改造的合理化建议。

4.1.2.8 应具备 OpenStack 云平台部署、运维能力，熟练掌握分布式存储、集中式存储等常见故障的分析和处理能力等。

4.1.2.9 建立服务机制应符合以下要求：

a) 服务热线：运维单位应具备固定客服电话，保持 7×24 小时处于接听状态；

b) 服务响应：日常技术咨询、技术支持等服务响应时间应小于 1 小时；应急维护的服务响应时间应小于 1 小时；设备、系统发生故障时，运维单位应在与建设/使用单位约定的时间内恢复设备、系统正常运行；

c) 维保回访：应在每次维护保养任务完成后 3 天内，对用户进行跟踪回访；

d) 投诉受理：接到用户投诉后，处理意见的反馈应不超过 2 天，投诉回复率 100%；

e) 用户满意度调查：用户满意度调查六个月内应不少于 1 次。评分项目包括服务态度、服务技能、响应时间、用户需求理解率、回访跟踪时效、结果满意度等。

4.1.3 软件原厂支持服务

软件原厂技术支持服务应满足以下要求：

a) 原厂技术支持提供不限于远程技术支持、电话技术支持、现场技术支持服务；

b) 原厂技术支持有义务为针对云平台组织实施的二次开发提供技术支持服务；

c) 原厂技术支持有义务配合运维方提供紧急情况下应急响应支持服务。

4.1.4 服务等级

运维单位应实施分级服务管理，服务水平通常可分三级，一级为最高等级。服务等级不同，维护保养单位对建设/使用单位提供的服务质量与维护费用价格也不同，SLA指标见表1。

表 1　SLA 指标

序号	指标	描述	单位	参考数据	服务等级	参考价格
1	事件平均响应时间(T)	事件响应总时间/事件次数	分钟	T≤30	一级	P*1.1
				30＜T≤60	二级	P
				60＜T≤90	三级	P*0.95
2	事件按时解决率(S)	事件按时解决次数/事件总次数	百分比	S≥95%	一级	P*1.1
				90%＜S≤95%	二级	P
				S＜90%	三级	P*0.95
3	事件响应超时率（O）	事件响应超时次数/事件总数	百分比	O＜5%	一级	P*1.1
				5%＜S≤10%	二级	P
				S＞10%	三级	P*0.95
4	事件平均客户满意度(G)	事件平均客户满意度=∑满意度/统计次数	百分比	G≥95%	一级	P*1.1
				90%＜G≤95%	二级	P
				G＜90%	三级	P*0.95

4.2 运维服务流程

4.2.1 云平台运维服务流程

云平台运维流程应按照图 1 的程序进行：

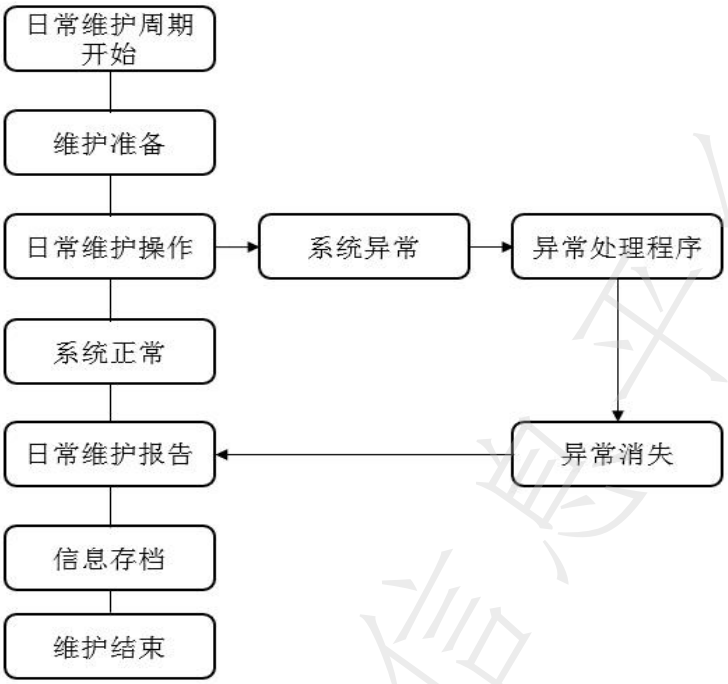

图 1　云平台运维流程图

4.2.2　云平台日常巡检工作流程

云平台日常巡检工作流程应按照图 2 的程序进行：

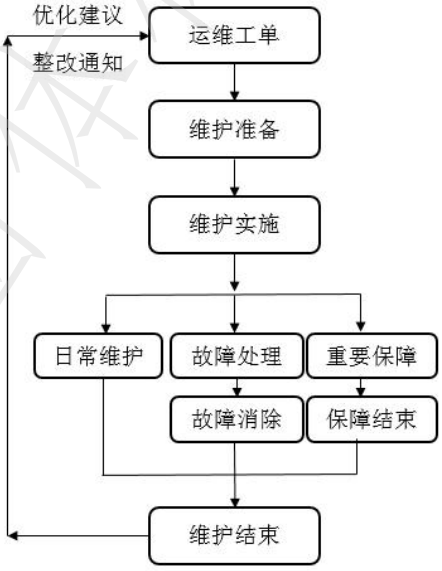

图 2　云平台日常巡检工作流程图

4.2.3　故障处理工作流程

故障处理流程应按照图3的程序进行：

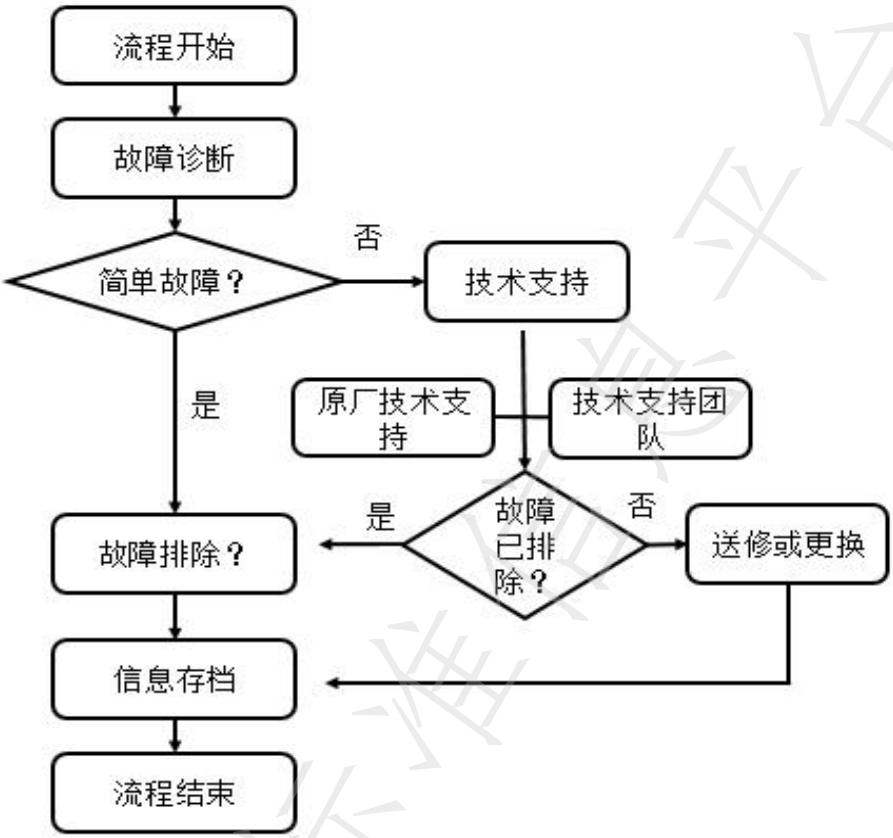

图3　故障处理流程图

4.3　日常巡检

4.3.1　物理硬件巡检

4.3.1.1 服务器巡检主要检查应符合以下内容：

a) 检查服务器电源线、网线等是否连接可靠；

b) 检查服务器面板指示灯是否存在异常报警；

c) 检查服务器日志是否存在红色高危报警信息，日常频繁硬件报错信息；

d) 检测服务器系统是否存在高危漏洞，高危补丁等；

e) 通过专业第三方硬件诊断工具检测硬件综合运行信息。

4.3.1.2 网络设备巡检应包含以下内容：

a) 检查设备网线、跳线等是否连接可靠；

b) 检查设备故障灯是否闪亮或常亮；

c) 检查网络设备是否存在高危端口、漏洞等；

d) 登录设备，审计设备运行日志，诊断设备是否存在运行故障；

e) 路由器、交换机等设备。

4.3.1.3 存储设备巡检应包含以下内容：

a) 检查存储设备所有硬盘是否正常工作；

b) 检查故障指示灯是否存在异常报警；

c) 检查存储设备容量是否达到设定阈值；

d) 检查设备运行日志，及时排查潜在故障；

e) SAN 存储、NAS 存储、分布式存储等设备。

4.3.1.4 安全设备巡检应包含以下内容：

a) 安全设备日常风险性评估；

b) 安全设备日常安全性加固；

c) 安全设备系统运行状态信息收集及分析；

d) 安全设备攻击防范事件信息收集及分析；

e) 安全设备病毒库日常监测和更新；

f) 物理防火墙、安全审计设备、入侵防护设备等。

4.3.2 软件巡检

4.3.2.1 操作系统巡检应包含以下内容：

a) 操作系统漏洞扫描与更新；

b) 操作系统运行日志收集与审计；

c) 操作系统日常数据备份；

d) 操作系统开机项、注册表项、进程项异常情况处理；

e) 操作系统计算、存储、网络等资源使用情况分析，及时在阈值前做出响应。

4.3.2.2 运行软件巡检应包含以下内容：

a) 高危软件、高危工具排查和清理；

b) 软件运行日志收集和排查；

c) 软件更新和新版本运行环境测评；

d) 软件系统、数据日常备份工作。

4.3.2.3 **云平台巡检应包含以下内容：**

a) 云平台资源池状态日常监控和扩容建议；

b) 云平台组件（资源池、云数据库、云镜像仓库、云安全组件等）可用性情况；

c) 云平台虚拟机状态日常监控；

d) 云平台运行日志收集和排查；

e) 云平台告警监控和处理。

4.3.3 云平台巡检内容基本架构如图 4 所示。

图4 云平台巡检基本架构图

4.3.4 自动巡检应满足以下要求：

a) 自动收集资源池使用状态，实时完成收集；

b) 自动收集网络实时流量，自动分析网络延迟性；

c) 实时监控并推送异常流量；

d) 云平台系统告警、软件告警实时推送；

e) 云平台软件、硬件故障代码及故障实时推送。

4.4 故障处理

4.4.1 处理原则

故障处理应遵循尽可能减少业务的中断时间、尽可能地恢复业务和尽可能减少平台与用户数据的丢失的原则，是公共安全视频监控云计算平台业务连续性、业务恢复和业务重续三大问题重要解决办法与保障手段。

4.4.2 处理措施

4.4.2.1 运维单位应根据故障级别，采取必要的服务措施，尽快修复故障，恢复系统正常运行。运维方必须保证优先实施业务恢复，在恢复业务的前提下，再进行彻底地故障修复。

4.4.2.2 故障级别由低到高分为：

a) 三级故障（仅为个别节点不能访问但不影响整个云平台的功能）；

b) 二级故障（云平台的某些功能受损但日常应用基本可维持）；

c) 一级故障（云平台功能受重大影响或系统瘫痪）。

4.2.2.3 应根据故障的严重程度和影响程度的不同，将各种云平台故障和告警进行分级处理，故障处理要求见表 2。

表 2 故障处理要求

序号	等级	故障描述	响应时间	达到现场时间	故障恢复时间
1	一级	云平台崩溃导致大范围系统和设备停止运行，数据丢失等故障	＜30 分钟	1 小时	2 小时
2	二级	云平台部分功能模块失效、系统性能下降，但能正常运行	＜30 分钟	2 小时	4 小时
3	三级	云平台或平台内部功能模块报错或警告，但系统和设备能继续运行且性能不受影响	＜60 分钟	2 小时	4 小时

4.4.2.4 故障维修及反馈记录表见下表3。

表 3 故障维修及反馈记录表

设备/设施/系统名称		型号/序列号	
位置		子分部/系统名称	
运维单位名称			
故障现象描述			
故障原因分析			
维修步骤			
维修结果及反馈意见			
客户评价			
维修人	签字： 年 月 日	运行负责人	签字： 年 月 日
注：故障处理后，运维方应出具故障维修及反馈记录表，书面形式记录本次故障，并将故障完整记录至运维知识库。			

4.4.3 **考核指标**

云平台硬件设备及软件的24小时故障修复率必须达到100%。

24小时故障修复率=（24小时内修复的故障次数合计/故障总次数）×100%。

4.5 应急响应

4.5.1 应急准备

4.5.1.1 应急响应组织建设应满足以下要求：

a) 应急响应组织的人员应属于运行维护服务组织的人员，也可包括原厂技术支持等其他机构的专家和人员。

b) 应规定运行维护服务及应急响应所有相关利益方的角色及职责，并为关键角色提供备选人选。同时角色和职责应做如下明确要求：

①应急响应责任者：可由运维方信息化部门最高管理者担任，统筹协调应急响应工作；

②现场负责人：由应急响应责任者授权，负责应急事件监测与预警、应急处置等现场工作；

③分组负责人：可在组织内成立多个分项小组并设定负责人，承担应急响应中各专业性工作；

④值班人员：组织内承担现场值守工作的人员；

c) 应明确应急响应服务的范围、要求等，并确定沟应急响应的通流程和方式和形成书面记录；

d) 运行维护过程中运维方涉及组织和人员的变更应与相关利益方达成一致，并形成记录；

e) 应建立对应急响应组织内人员的考核机制，明确考核指标及方法。考核至少每年进行一次，以确保组织育能持续满足应急响应要求。

4.5.1.2 视频监控云平台应急响应制度应满足以下要求

a) 云平台拥有方和运维方就应急响应制度达成一致，共同遵守；

b) 云平台拥有方定期对应急响应制度进行评审，云平台运维方根据评审进行改进；

c) 在云平台组织战略、业务流程、客户要求等发生重大变化时对应急响应制度进行调整。

4.5.1.3 视频监控云平台应急响应组织应根据应急事件级别制定应急响应预案，内容应包括：

a) 应急响应预案的编制目的、依据和适用范围；

b) 应急响应预案具体的组织体系结构及人员职责；

c) 应急响应预案的监测和预警机制；

d) 应急事件级别及对应的处置流程、方法；

e) 应急事件响应的资源、技术保障措施。

4.5.2 监测与预警

4.5.2.1 日常监测的职责及范围包括

a) 对云平台运行环境、云平台安全设备、云平台网络设备、云平台系统等运行维护服务对象的运行情况进行监测与预警，跟踪和判别设备容量、可用性和连续性；

b) 组织应对信息系统所承载的业务数据进行监测，跟踪和判别业务数据是否超出了预警条件。

4.5.2.2 记录与报告的内容包括

a) 应急事件发生及发现的时间、位置；

b) 应急事件现象及影响范围描述；

c) 应急事情初步原因分析。

紧急事件产生时，驻场值班人员应按照约定的形式第一时间间隔上报现场负责人。发现应急事件时，值班人员应提交报告。

应急事件报告应及时提交给现场负责人。同时，值班人员应采取必要措施，开展应急事件的先期处置，以提高应急响应效率，避免次生、衍生事件的发生。

4.5.2.3 应急事件演练的内容及要求应包括：

a) 预先制定应急演练计划、演练脚本，并征得视频监控云平台应急响应组织负责人批准；

b) 应急演练的整个过程应有详细的记录，并形成详细书面报告；

c) 应急演练不能影响业务的正常运行。

为检验应急响应预案的有效性，同时使相关人员了解运行维护预案的目标和内容，熟悉应急响应的操作规程，组织应周期性进行应急演练。

4.5.3 应急处置

4.5.3.1 视频监控云平台应急响应组织接到紧急事件报告后，应按照应急事件响应预案，开展包括人员、资金和设备等统一的应急调度，应急调度中应：

a) 迅速组织必要人员进行事件勘察、分析；

b) 下达应急事件调度命令并保持跟踪；

c) 保护紧急事件现场可追查的相关线索。

4.5.3.2 排查与诊断流程应包含以下要求：

a) 现场处置人员可借助各类排查诊断分析工具，如应用软件、电子分析工具、故障排查知识库等进行现场故障排查；

b) 现场处置人员进行故障排查和诊断，必要时可寻求组织其他人员以现场或远程方式进行支持；

c) 现场处置人员应随时向现场负责人汇报故障排查情况、诊断信息、故障定位结果等；

d) 现场处置人员应将排查与诊断的过程与结果信息进行整理与归档。

4.5.3.3 处置过程中，现场负责人应及时与相关利益方进行沟通，沟通的内容主要包括系统故障点、造成故障的原因、排查诊断状况等，并及时组织相关利益方对问题进行确认。

4.5.3.4 视频监控云平台事件应急响应处理与恢复的原则包括:

a) 应急事件处理过程中，采用的方法、手段不应造成次生、衍生事件的发生；

b) 应急事件处理过程中，必要时可启用备品备件、灾备系统等；

c) 现场负责人应组织对应急事件处理与恢复的结果进行初步确认；

d) 应对应急事件处理过程及结果信息进行记录，并及时告知相关利益方。

基于应急响应预案、配置管理数据库、知识库等进行故障处理和系统恢复，在满足事件级别处置时间要求的前提下，尽快恢复服务处理与恢复。

4.5.4 持续改进

4.5.4.1 应急工作分析

应急工作分析应从以下方面推进：

a)应急响应工作的绩效；

b)应急准备工作的充分性和有针对性；

c)应急事件处置的经验得失；

d)信息系统中潜在的类似隐患。

4.5.4.2 应急工作改进

应急工作改进应明确如下要求：

a) 明确云平台改进目标、持续优化场景等，并根据目标制定对应的具体工作计划；

b) 评估云平台改进所需的各种资源，包括人员、资金和设备等；

c) 和云平台拥有方、原厂技术支持方保持持续性闭环互动，根据新的需求或技术持续推进改进工作。

4.5.4.3 应急工作总结

a) 视频监控云平台应急响应组织应定期对应急响应工作进行持续改进，分析总结经验教训，并采取适当的后续措施，杜绝类似事件再次发生，提升云平台运行稳定性；

b) 应急事件总结、应急工作审核的结果应该作为应急准备阶段各项工作的改进要素；

c) 视频监控云平台应急响应组织应根据总结报告中给出的建议项和评审结果，完善信息系

统，深化应急准备工作，持续提升云平台抗击风险能力。

4.6 软、硬件维护

4.6.1 硬件维修与更换

运维单位对云平台服务器、网络设备、存储设备等硬件设施进行维修或更换服务，必须满足如下条件，方可进行下一步操作：

a) 书面形式告知使用单位硬件维护将造成业务停机时间、并征得使用单位同意；

b) 所更换的部件备件已采购完成，并以确认兼容性；

c) 所维修的部件维修方案等以获得厂商或技术人员认同。

硬件维修、更换完成后，运维方应及时恢复云平台自身业务，并告知和配合使用方完成使用方业务恢复，同时，维护完成后应配合填写硬件维修、更换记录表，以书面形式记录本次维修、维护记录。硬件维修、更换记录表如表4所示：

表4 硬件维修、更换记录表

设备/设施/系统名称		型号/序列号	
位置		子分部/系统名称	
运维单位名称			
维修、更换现象描述			
更换部件信息及数量			
更换、维修步骤			
维修结果及反馈意见			
客户评价			
维修人	签字： 年 月 日	运行负责人	签字： 年 月 日

4.6.2 软件维护服务

软件维护服务应满足以下要求：

a) 首次软件维护，运维方需在软件原厂完成软件部署验收通过，并完成交接后方可进行；

b) 软件维护前，需要对软件配置、环境变量、系统数据、业务数据等重要部分进行备份操作

c) 软件维护服务过程中，需保障在不影响当前业务运行；

d) 软件维护如若涉及当前业务停止，需提前通过书面形式告知云平台使用方，并征得云平台使用方同意。

4.7 运维报告

运维报告有助于运维方对云平台运维工作全方位掌控，帮助运维方完善运维工作量评估和提供决策性云平台运行数据判断；有助于云平台拥有方完整掌握云平台运行状态，故运维方一线工作人员必须提供运维报告。运维报告分为运维周报和运维月报，运维周报见表5，运维月报见表6。

表5 运维周报

部门		姓名		日期	
本周工作进展					
问题分析	分析列表	问题原因	解决方案		备注
下周工作安排					
部门主管意见					

表6 运维月报

部门		姓名		日期	
当月总结					
本月总体运行情况	云平台基础环境运维情况				
	云平台系统运维情况				
	业务系统运维情况				
上月问题解决措施和落实情况	故障原因分析				
	故障解决措施				
	故障跟进闭环				
巡检报表汇总分析	巡检日报汇总及分析				
	巡检周报汇总及分析				
当月重点故障分析	重大故障汇总				
	重大故障解决措施				
	重大故障跟进闭环、归档				

	现场重点情况说明	
下月工作计划		
主管部门意见		

4.8 运维考核

4.8.1 考核项目及目标如下：

a) 事件平均响应时间=事件响应总时间/事件次数，合格值为≤60分钟；

b) 事件按时解决率=事件按时解决次数/事件总次数，合格值为95%；

c) 事件响应超时率=事件超时次数/事件总次数，合格值为≤10%；

d) 事件平均客户满意度=事件满意次数/事件总次数，合格值为95%。

4.8.2 考核满分总分100分，通过在线考核及人工抽查的方式进行，月考核得分=事件平均响应时间得分 +事件按时解决得分+事件响应超时率得分+事件平均客户满意度得分。全年得分为每月的平均得分。

4.9 运维资料管理

运维单位应定期提交视频监控云平台运维巡检相关资料，巡检内容至少包含交换机巡检模板（见表7、表8）、防火墙巡检模板（见表9、表10），路由器巡检模板（见表11、表12），服务器巡检模板（见表13、表14），存储巡检模板（见表15），云平台巡检模板（见表16、表17、表18、表19、表20）。

表7 交换机巡检表A

	设备名称	设备型号	硬件运行状态	软件运行状态	检查方式
网络设备	交换机		□正常 □不正常	□正常 □不正常	
			□正常 □不正常	□正常 □不正常	
			□正常 □不正常	□正常 □不正常	

表8 交换机巡检表B

检查项目	检查子项目	检查结果	说明	分析结果
设备指示灯检查	主控板指示灯检查			□合格 □不合格 □不涉及
	业务板指示灯检查			□合格 □不合格 □不涉及
电源\风扇状态检查	电源\风扇检查			□合格 □不合格 □不涉及
异常告警检查	告警记录察看			□合格 □不合格 □不涉及
设备性能检查	CPU 利用率			□合格 □不合格 □不涉及

	内存利用率			□合格 □不合格 □不涉及
端口信息检查	端口信息检查			□合格 □不合格 □不涉及
路由信息检查	路由信息检查			□合格 □不合格 □不涉及

表9　防火墙巡检表A

	设备名称	设备型号	硬件运行状态	软件运行状态	检查方式
网络设备	防火墙		□正常 □不正常	□正常 □不正常	
			□正常 □不正常	□正常 □不正常	
			□正常 □不正常	□正常 □不正常	

表10 防火墙巡检表B

检查项目	检查子项目	检查结果	说明	分析结果
设备指示灯检查	主控板指示灯检查			□合格 □不合格 □不涉及
	业务板指示灯检查			□合格 □不合格 □不涉及
电源\风扇状态检查	电源\风扇检查			□合格 □不合格 □不涉及
异常告警检查	告警记录察看			□合格 □不合格 □不涉及
设备性能检查	CPU 利用率			□合格 □不合格 □不涉及
	内存利用率			□合格 □不合格 □不涉及
调试开关关闭	调试开关关闭			□合格 □不合格 □不涉及
端口信息检查	端口信息检查			□合格 □不合格 □不涉及
安全策略检查	安全策略配置检查			□合格 □不合格 □不涉及
拦截记录检查	拦截记录检查			□合格 □不合格 □不涉及

表11　路由器巡检表A

	设备名称	设备型号	硬件运行状态	软件运行状态	检查方式
网络设备	路由器		□正常 □不正常	□正常 □不正常	
			□正常 □不正常	□正常 □不正常	
			□正常 □不正常	□正常 □不正常	

表12　路由器巡检表B

检查项目	检查子项目	检查结果	说明	分析结果
设备指示灯检查	主控板指示灯检查			□合格 □不合格 □不涉及
	业务板指示灯检查			□合格 □不合格 □不涉及
电源\风扇模块检查	电源\风扇检查			□合格 □不合格 □不涉及
异常告警检查	告警记录察看			□合格 □不合格 □不涉及
设备接地检查	设备接地检查			□合格 □不合格 □不涉及
设备性能检查	CPU 利用率			□合格 □不合格 □不涉及
	内存利用率			□合格 □不合格 □不涉及
端口信息检查	端口信息检查			□合格 □不合格 □不涉及
路由信息检查	路由信息检查			□合格 □不合格 □不涉及

表13　服务器硬件巡检表

检查项	检查操作	参考标准	巡检情况
机柜或者机器上的防尘网	观察机柜以及机器上的防尘网上的灰尘	是否在防尘上堵塞导致气流不畅	
系统风扇运转检查	观察并用手感觉进风和出风是否正常	主机和磁盘柜的所有风扇运转正常	
服务器硬盘工作状态	硬盘指示灯指示是否正常，一般绿色为正常	绿色闪烁	
服务器散热检查	靠近服务器检查是否有热风吹出		
服务器电源连接检查	电源连接线是否有松动、接触不良等情况		
服务器机房温\湿度	机房温\湿度是否异常变动，温度数值多少	参考值温度：20℃-26℃ 参考值湿度：45%-60%	
服务器机房静电防护	防静电地板是否损坏，防静电设备是否正常		
服务器标签检查	标签是否松动、脱落，字体是否模糊不清		

表14　服务器系统及安全巡检表

检查项	检查操作	参考标准	巡检情况
操作系统版本检查	执行命令 uname -a		
系统账号检查	利用 root 身份、口令登录	能够正常登录到系统	
系统运行状态	uptime	系统 UP 时间应该为上次重启到目前的时间	
检查各进程资源占用率	top -c	资源使用率小于 80%	
进程占用资源检查	top -c 进程名	查看系统最占资源的进程	
检查当前登录用户	who	除了管理员外没有其他用户登录	
文件系统占用率	df -ah	没有文件系统超过 80%的现象	
文件系统日志	dmesg	无错误日志或错误日志不会影响系统的正常运行	
系统登录情况检查	lastlog	无异常账户或异常事件登录	

表15　存储巡检表

检查项	检查结果		备注
1.通过 CAP2 检查磁盘有无故障？(Hard error)	正常 □	异常 □	
2.通过 CAP2 和 SPLAT，检查有无其他报错？如 health-checkfailed,磁盘的 soft error 等	正常 □	异常 □	
3.检查磁盘柜每个 LCC 风扇\电源状态：	正常 □	异常 □	
4.检查每个 SPS 状态：	正常 □	异常 □	
5.检查 SPS 的 Cabling 是否有效？	正常 □	异常 □	
6.检查两个 SP 所有 Port 是否都 Online?	正常 □	异常 □	
7.检查是否每个 SP 的 read cache\write cache 已处于 enable 状态？	正常 □	异常 □	
8.检查是否每块 HBA 连接到存储的路径都能正常 login 和 register？	正常 □	异常 □	
9.检查 HA cache vault 是否已被 enable?	正常 □	异常 □	

4.9.1 云平台巡检模板

4.9.6.1 主机巡检

每日主机巡检报表见表16：

表16 主机每日巡检表

巡检员			联系方式			日期		
项目类别	主机状态	CPU 利用率	磁盘利用率	内存利用率	内网流量状况		外网流量状况	
					均值	峰值	均值	峰值
主机								

4.9.6.2 云组件巡检

每日云组件巡检报表见表17：

表17 云组件每日巡检表

巡检员		联系方式		日期	
项目类别		监控项		可用值	可用率%
云组件		存储资源池			
		计算资源池			
		SDN 网络资源池			
		云数据库			
		镜像仓库			
		云安全组件			

4.9.6.3 云服务巡检

每日云服务巡检报表见表18：

表18　云服务每日巡检表

巡检员		联系方式		日期	
项目类别		监控项		可用率%	
云服务		弹性计算服务			
		负载均衡			
		云编排服务			
		云监控			
		弹性伸缩			
		关系数据库			
		简单通知服务			
		对象存储服务			
		自助服务平台			

4.9.6.4 存储设备巡检

每日存储设备巡检报表见表19：

表19　存储设备每日巡检表

巡检员		联系方式		日期	
项目类别		监控项		可用率%	
云存储设备		集中式存储			
		本地文件系统			
		本地逻辑卷			
		分布式存储			

4.9.6.5 云平台警报巡检

每日警报巡检报表见表20：

表20　云平台每日警报巡检表

巡检员		联系方式		日期	
项目类别		监控项		可用率%	
报警		实例			
		存储卷			
		负载均衡			
		主机			
		区域			
		服务			
		弹性组			

4.10 运维知识库

运维知识库管理应满足如下条件：

a) 建立完整运维知识库结构和数据管理结构；

b) 建立完整运维知识库运行流程和状态跟踪；

c) 建立完整运维知识库录入流程。

5 云平台安全

5.1 云平台的物理安全

5.1.1 主机安全应包括以下内容：

a) 系统上线前，应进行全面的主机安全评估和安全加固，并遵循安全最小化原则，关闭未使用的服务组件和端口；

b) 应对主机系统（包括：虚拟机管理器、操作系统、数据库系统等）定期评估。补丁更新前，测试与现有系统的兼容性；

c) 应对操作系统文件、进程、注册表、服务、账户进行强制访问控制；

d) 应具备实时检测和查杀病毒、恶意代码等服务，并保持防病毒代码的更新，能够及时发现主机异常行为；

e) 应定期对云服务器上运行的端口、账号的变动情况进行记录，自动发现资产异常情况；

f) 应定期对常见登配置进行检查，能够发现服务是否使用了弱口令；

g) 应定期自动检测操作系统中存在的安全漏洞，并提供补丁修复建议；

h) 应对用于主机系统用户的身份进行鉴别，包括多种身份鉴别方式、多因子认证、单点登录；

i) 应限制匿名用户的访问,设置单一用户并发连接次数、连接超时限制，并采用最小授权原则；

j) 应采用校验技术或密码技术保证通信过程中数据的完整性；

k) 应采用密码技术保证通信过程中数据的保密性；

l) 应在通信前基于密码技术对通信的双方进行验证或认证；

m) 应使用国家密码主管部门颁布的相关标准密码算法。

5.1.2 平台安全应包括以下内容：

a）应构建云防御体系，依托云化安全资源，对网络层访问控制、流量监控及威胁检测，实现对云数据中心外部边界的风险收敛及网络安全防护；

b）应通过云安全管理平台提供安全服务，实现对云服务交付层的系统级安全管理和安全运行支撑；

c）云安全管理平台应通过三权分立管理，构建云特权操作管控系统、平台特权操作管控系统，开展特权用户操作和访问控制，有效管控和降低资源管控、运行维护等操作的安全风险；

d）应构建云虚拟化层安全防护，适配主流虚拟化平台，对云平台虚拟化层进行检测及防护，有效防御云内横向攻击，并基于底层调优机制，降低安全检测的开销；

e）应建设云网隔离机制，通过区域划分、路由策略、动态引流等方式实现网络安全引流，云安全资源池实现面向各应用系统区内部网络、容器网络的网络访问控制；

f）应通过云安全管理平台，提供统一的控制平面，支撑对混合云、多云异构环境下的全局安全策略管控；

g）云安全管理平台应支持多租户的架构，使得系统不仅适合私有云的部署，也适合提供租赁服务的公有云。通过管理中心，可以为每个用户配置不同的安全策略。

5.2 云平台的数据及网络安全

5.2.1 数据安全应包括以下内容：

a) 应监视并记录对数据库服务器的各类操作，通过对网络数据的分析，实时解析，并记入审计数据库中。实时监测并分析、还原各种数据库操作过程。对数据库系统漏洞、登录帐号、登录工具和数据操作过程进行跟踪，及时发现对数据库系统的异常使用。定期统计审计报表。实现对数据库系统操作的监控和审计；

b) 基于IP 地址、MAC 地址、用户、应用程序、时间等因子对访问者进行身份认证，形成多因子认证；

c) 应用程序对数据库的访问，须经过两层身份认证；

d) 应实时检测数据库SQL 注入和缓冲区溢出攻击。并报警或者阻止攻击行为，同时详细的记录攻击操作发生的时间、来源IP、用户名、攻击代码等信息；

e) 应有数据存储安全措施，备份/恢复机制，传输安全以及对敏感信息的安全机制。

5.2.2 网络安全应包括以下内容：

a) 应对实时流量数据采集,基于源地址/地区、目的地址/地区、服务、例外应用、时间等多种方式进行流量采集；

b) 应能对流量数据外发。支持恶意样本外发；

c) 应能对流量还原。对单边、双向流量进行还原，生成流量日志并外发；

d) 应能对流量解密，能明文流量镜像。能添加SSL入站检查配置文件；

e) 应能通过流量进行资产识别。能够基于资产流量特征，有效识别资产类型；

f) 应通过流量进行应用识别。并能够手动自定义应用识别签名；

g) 应具备旁路阻断能力。旁路IP阻断、旁路URL重定向、旁路DNS重定向；

h) 应具备安全诊断能力。能基于IP、URL、应用条件抓包。抓取TCP包和UDP包；

i) 应具备恶意文件检测能力，对多种协议应用数据包进行恶意文件检测。对恶意文件留存和PCAP抓包留存本地；

j) 应能通过流量对漏洞和黑客软件进行检测；

k) 应能进行入侵检测处理。针对具体的漏洞或黑客软件的攻击类型进行日志、放行、重置方式的动作设定；

l) 应能进行异常流量检测；

m) 应能进行流量DDoS检测。

5.3 人的行为安全应包括以下内容：

a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

b) 应通过安全管理员对联网接入网关、边界安全网关等重要系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等；

c) 应对重要安全运营人员的工作就位、工作状态情况进行检视；

d) 应对重要安全运营工作的进展情况及遇到的困难点进行检视，并协调资源保障工作进展和结果。

e) 应对巡检人员、时间、内容等进行详细记录，形成巡检记录表，以备后续审查；

f) 应制定供应商以及外包运维人员对云平台系统的巡检安全管理制度；

g) 应制定培训计划，对安全运营人员进行持续化培训，包括对不同安全运营人员进行安全运营基础知识、安全风险管理、渗透测试、风险评估、安全运营平台管理、岗位操作规程等专项培训；

h) 应定期对不同岗位的人员进行技能考核，评估专项技能和岗位要求技能的差距。

6 费用核准方法

6.1 云平台建设费用

6.1.1 云平台硬件费用估算

云平台硬件费用包含服务器、交换机等计算、网络设备，云平台建设硬件费用估算，应由云平台拥有方提出云平台建设规模，云平台运维方及硬件供应厂商根据建设规模共同评估硬件需求数量。硬件需求数量评估在征得设计院、第三方技术团队、第三方专家团队等任何拥有评估实力团队对可行性评估后，由云平台建设方向硬件供应商以不高于武汉市物价局核定市场价格采购。

6.1.2 云平台虚拟化软件费用估算

计算方式: 云平台虚拟化软件费用＝CPU总颗数×单颗CPU授权费

注：CPU授权费用根据厂家实际出厂定价，不高于武汉市物价局核定的市场价。

6.1.3 云平台实施费用

云平台实施费用约为整个云平台建设费用5%-10%之间，具体数值根据云平台实施方针对云平台实施方案、交付计划、培训计划、验收计划、交付效率等值共同评估，每项不达标或未提供扣1%，最高为10%，最低不低于5%。

6.1.4 数据中心机柜租赁费用

计算方式：数据中心机柜租赁费用＝机柜数量×单柜费用

注：单柜费用根据数据中心级别和机柜功率计费。具体计费方式参照武汉市IDC机柜租用近三月平均数值)×企业系数。企业系数由数据中心机柜拥有方和数据中心机柜租赁方根据数据中心等级、可靠性、运维能力、额外服务等条件共同评估。

6.1.5 安全资源池费用

安全资源池各厂商差别较大，建议按实际情况定价。

6.1.6 培训费用

按培训内容和培训次数，单独收费。

6.2 迁移上云费用

云平台迁移上云费用指运维方协助云平台使用者将现有业务从本地迁入云平台所产生的费用，根据主机数量、业务数量、数据总量形成的工作量评估，具体评估方式为：

计算方式：迁移上云费用=业务量所需人数×每人每月费用

注：每人每月费用为武汉市IT人员平均月薪×企业系数。企业系数由云平台运维方根据运维场合条件、福利、运维企业福利等综合评估，与云平台拥有方共同核准。

6.3 云平台运维费用

6.3.1 运维人员支出费用

运维人员开支费用根据云平台规模和要求评估总需运维人员。

计费方式：运维人员开支费用＝总需运维人数×武汉市IT人员平均月薪×企业系数

注：企业系数由云平台运维方根据运维场合条件、福利、运维企业福利等综合评估，与云平台拥有方共同核准。

6.3.2 运维材料支出费用

运维材料支出费用根据云平台运维过程中实际使用材料计费，运维方在运维过程中有更换配件、新增配件的需求，必须填写材料用料单，运维完成后根据材料用料单进行费用结算。