ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB XX/T XXXX—XXXX

云计算平台运行维护 云资源监控实施指南

Operation and maintenance of cloud computing platform-Implementation guide for cloud resource monitoring

（征求意见稿）

（本草案完成时间：2022-8-21）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：辽宁省工业和信息化发展研究院、国网辽宁省电力有限公司信息通信分公司、辽宁职业学院、沈阳化工大学、本溪钢铁（集团）信息自动化有限责任公司、联通（辽宁）产业互联网有限公司、鞍钢数智科技（辽宁）有限公司。

本文件主要起草人：姜胜海、刘晓强、吴庆、王姝、李博文、张帅、冯陆、高洋、张雪、刘洋等。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市北陵大街45-2号，联系电话：024-86913384

本文件起草单位通讯地址：沈阳市和平区太原北街2号综合楼A座10层，联系电话：024-88785218

云计算平台运行维护 云资源监控实施指南

1 范围

本文件规定了云计算平台运行维护过程中云资源监控的实施指南，包括监控指标体系、监控方法、监控频率、告警管理等方面的要求。本文件适用于辽宁省内各类云计算平台的运行维护管理，涵盖公有云、私有云和混合云等不同部署模式的云计算平台。

本文件旨在为云计算平台运营单位提供一套规范、统一的云资源监控实施标准，确保云计算平台的稳定运行，提高资源利用效率，及时发现和解决潜在的问题，保障业务连续性。

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 37938—2019信息技术云资源监控指标体系

GB/T 37736—2019信息技术云计算云资源监控通用要求

GB/T 31167—2023信息安全技术云计算服务安全指南

GB/T 31168—2023信息安全技术云计算服务安全能力要求

GB/T 37739—2019信息技术云计算平台及服务部署要求

GB/T 37972—2019信息安全技术 云计算服务运行监管框架

3 术语和定义

下列术语和定义适用于本文件。

3.1

云计算平台 cloud computing platform

提供云计算服务的基础设施和软件系统的集合，包括计算、存储、网络、安全等资源，以及相应的管理和调度机制。参考国家标准中的定义，并结合辽宁省实际应用场景，强调云计算平台在本地的应用特点和重点关注方面。

3.2

云资源 cloud resources

云计算平台中可供使用的各种计算、存储和网络资源，包括物理资源和虚拟资源。对物理资源和虚拟资源分别进行详细解释，明确其涵盖的具体内容，如物理服务器、存储设备、网络设备以及虚拟机、虚拟网络等。

3.3

监控 monitor

对云计算平台中的云资源进行实时或定期的数据采集、分析和处理，以获取资源的使用状态和性能指标，并及时发现异常情况的过程。阐述监控在云计算平台运行维护中的重要性和作用机制。

4 总则

在本文件中，物理资源监控指标监控的对象是提供基础设施能力类型的云服务所需要的资源,包括物理服务器、存储设备、网络设备等。虚拟资源监控指标监控的对象是提供平台能力类型的云服务所需要的虚拟资源，包括虚拟机、虚拟网络等虚拟资源。应用服务监控指标监控的对象是提供应用能力类型的云服务所需要的资源，包括各类应用系统。

本文件中对云资源的监控通用要求包括技术要求和管理要求。如图1所示,监控技术要求从云服务提供者角色和云服务客户角色出发,针对物理资源监控指标、虚拟资源监控指标、应用服务监控指标分别提出相应要求。

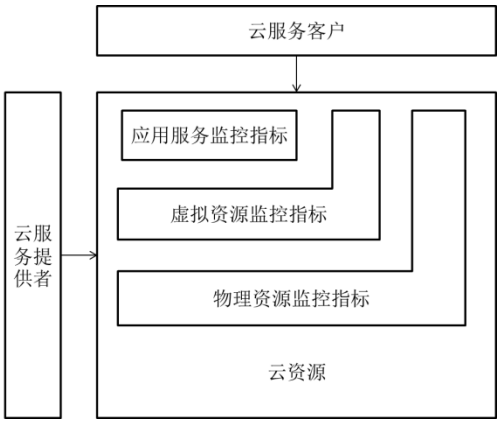

图1　云资源监控指标技术要求框架

5　监控指标体系

5.1　物理资源监控指标

5.1.1　服务器

服务器主要应包括：

a) CPU使用率：定义为服务器CPU在某一时间段内处于繁忙状态的时间比例。正常范围一般在0%-80%（可根据服务器配置和业务需求进行调整），当使用率超过设定的告警阈值（如90%）时，可能表示服务器负载过高，需要进一步分析原因，如是否存在大量计算任务同时运行或某个应用程序出现异常；

b) 内存使用率：指服务器内存被占用的比例。正常范围通常在0% - 70%左右，告警阈值可设为80%。过高的内存使用率可能导致系统性能下降，出现内存溢出等问题；

c) 磁盘I/O速率：反映磁盘读写数据的速度。单位通常为MB/s或KB/s，正常范围因磁盘类型和业务需求而异，一般来说，对于机械硬盘，顺序读写速率在几十MB/s到上百MB/s之间，随机读写速率较低；对于固态硬盘，顺序读写速率可达数百MB/s甚至更高。当磁盘I/O速率低于正常范围下限或高于上限时，可能表示磁盘存在故障或负载过高；

d) 网络带宽利用率：表示网络接口实际使用的带宽与总带宽的比值。正常范围一般在0% - 70%，超过80%可能意味着网络出现拥堵，需要检查网络设备和应用程序的网络使用情况；

e) GPU使用率：表示GPU当前工作负载的百分比，合理范围因使用场景而异。日常使用时，合理范围约为10%-30%，而游戏或专业应用时，70%-100%是正常的。使用率过高可能指示系统运行重负载任务或存在故障，可能导致性能问题；使用率过低则可能意味着GPU未被充分利用或驱动程序有问题，影响系统配置适宜性；

f) 磁盘使用率：指服务器磁盘被占用的比例。正常范围通常在0% - 90%左右，告警阈值可设为90%。过高的磁盘使用率可能导致数据丢失或无法写入新数据。

5.1.2 存储设备

存储设备应包括：

a) 存储容量使用率：计算存储设备已使用的容量与总容量的比例。当使用率在90%-100%时，需要及时扩展存储容量，以避免数据丢失或无法写入新数据；
b) 读写延迟：指从发出读写请求到完成读写操作所需要的时间。对于机械硬盘，读写延迟一般在几毫秒到几十毫秒之间；对于固态硬盘，读写延迟通常在零点几毫秒到几毫秒之间。异常的读写延迟可能表示存储设备存在故障或性能下降；
c) 每秒读写操作数（IOPS）：衡量存储设备每秒能够处理的读写操作次数。不同类型的存储设备IOPS差异较大，机械硬盘一般在几十到几百IOPS之间，固态硬盘则可达到数千甚至上万IOPS。如果IOPS低于正常范围，可能影响数据访问速度。

5.1.3 网络设备

网络设备应包括：

a) 端口流量：记录网络设备端口在某一时间段内传输的数据量。通过监控端口流量，可以了解网络负载情况，及时发现网络拥塞点；
b) 丢包率：指在网络传输过程中丢失的数据包数量与发送的数据包总数的比例。正常情况下，丢包率应极低（小于0.1%），较高的丢包率可能导致网络连接不稳定，影响业务运行；
c) 延迟时间：从发送数据包到收到响应数据包所需要的时间。网络延迟应保持在合理范围内，不同类型的网络应用对延迟的要求不同，如实时视频会议对延迟要求较高，一般应小于100ms；普通网页浏览延迟可适当放宽；
d) 带宽利用率：同服务器的网络带宽利用率，正常范围一般在0% - 70%，超过80%可能需要优化网络配置。

5.2 虚拟资源监控指标

5.2.1 虚拟机

虚拟机应包括：

a) CPU配额使用率：虚拟机所分配的vCPU资源在实际使用中的比例。正常范围可参考服务器CPU使用率，一般在0% - 80%，超过设定阈值可能影响虚拟机性能；
b) 内存分配量与使用量：分别记录虚拟机分配的内存容量和实际使用的内存容量。确保使用量不超过分配量，且内存使用率在合理范围内（如0% - 70%），否则可能导致虚拟机运行缓慢或出现内存不足的错误；
c) 虚拟存储容量使用率：计算虚拟机存储已使用的容量与总容量的比例。当使用率在90%-100%时，需要及时扩展虚拟机存储容量，以避免数据丢失或无法写入新数据；
d) 虚拟磁盘读写速率：反映虚拟机虚拟磁盘的读写数据速度。单位和正常范围可参考物理磁盘I/O速率，异常的读写速率可能影响虚拟机内应用程序的运行。

5.2.2 虚拟网络

虚拟网络应包括：

a) 虚拟网络带宽利用率：虚拟网络实际使用的带宽与总带宽的比值。正常范围一般在0% - 70%，过高的利用率可能导致虚拟网络拥堵，影响虚拟机之间的通信；
b) 虚拟交换机端口流量：类似于物理网络设备端口流量，用于监控虚拟交换机端口的数据传输量，以了解虚拟网络的负载情况。

5.3 应用服务监控指标

5.3.1 计算服务

计算服务应包括：

a) 作业提交成功率：指用户提交的计算作业成功进入计算队列并开始执行的比例。正常情况下，作业提交成功率应接近100%，较低的成功率可能表示计算服务存在问题，如作业调度器故障或计算资源不足；
b) 作业执行时间：从作业开始执行到完成所需要的时间。通过监控作业执行时间，可以评估计算服务的性能，对于不同类型的作业，执行时间可能有较大差异，应根据业务需求设定合理的参考范围；
c) 服务响应时间：用户发出计算服务请求到收到响应的时间。响应时间应尽可能短，一般对于交互式计算服务，响应时间应在几秒以内；对于批处理计算服务，响应时间可适当放宽，但也应在合理范围内。

5.3.2 存储服务

存储服务应包括：

a) 数据存储可靠性：通过数据冗余、备份恢复等机制来确保数据存储的可靠性。可通过定期检查数据一致性、备份完整性等方式来监控数据存储可靠性，要求数据存储可靠性达到较高水平（如99.99%以上）；
b) 数据访问成功率：用户请求访问存储数据成功的比例。正常情况下，数据访问成功率应接近100%，较低的成功率可能表示存储服务存在故障，如存储设备故障、网络问题或权限设置错误；
c) 备份恢复时间：从启动备份恢复操作到数据完全恢复可用的时间。备份恢复时间应在业务可接受的范围内，不同业务对备份恢复时间的要求不同，一般来说，关键业务的备份恢复时间应尽可能短。

5.3.3 网络服务

网络服务应包括：

a) 网络连接成功率：指网络连接建立成功的比例。正常情况下，网络连接成功率应接近100%，较低的成功率可能表示网络设备故障、网络配置错误或网络拥塞等问题；
b) DNS解析成功率：用户发出DNS查询请求到收到正确解析结果的比例。DNS解析成功率应接近100%，否则可能影响网络访问的正常进行。

6 监控方法

6.1 数据采集方法

6.1.1 基于代理的采集

基于代理的采集应包括：

a) 代理软件部署方式：在需要监控的物理服务器、虚拟机或其他设备上安装代理软件。代理软件应根据不同的操作系统和设备类型进行相应的配置和安装。例如，对于Linux服务器，可以通过包管理工具进行安装；对于Windows服务器，可使用安装向导进行安装；
b) 采集的数据类型和频率：代理软件可以采集多种数据类型，包括CPU使用率、内存使用率、磁盘I/O、网络流量等指标。采集频率可根据监控指标的重要性和变化频率进行设置。对于关键性能指标，如CPU使用率和内存使用率，可设置为每分钟采集一次；对于相对稳定的指标，如存储容量使用率，可设置为每小时采集一次。

6.1.2 无代理采集

无代理采集应包括：

a) 通过云计算平台自身的API或其他工具进行数据采集的方法：利用云计算平台提供的API接口，开发相应的采集程序或使用现有的工具来获取监控数据。例如，对于一些主流的云计算平台，如阿里云、腾讯云等，都提供了丰富的API接口，可用于获取各种资源的监控数据；
b) 优势：无代理采集不需要在被监控设备上安装额外的软件，减少了对设备的侵入性，降低了维护成本。同时，它可以更方便地获取云计算平台整体的资源信息，不受代理软件安装和配置的限制。

6.2 监控工具选择与配置

6.2.1 适合辽宁省云计算平台特点的监控工具列举

a) 开源工具：如Zabbix、Nagios等。Zabbix具有强大的监控功能，支持多种数据采集方式，能够对服务器、网络设备、虚拟机等进行全面监控；Nagios主要侧重于服务器和网络设备的监控，具有简单易用、配置灵活的特点；
b) 商业软件：如SolarWinds、Dynatrace等。SolarWinds提供了一套完整的IT管理解决方案，包括云资源监控功能，其界面友好，功能强大；Dynatrace专注于应用程序性能监控，同时也涵盖了云资源监控的相关内容，具有先进的数据分析和故障诊断能力。

6.2.2 监控工具的配置要点

a) 数据源配置：根据所选监控工具和采集方法，正确配置数据源。对于基于代理的采集，需要指定代理软件的安装位置和采集数据的存储位置；对于无代理采集，需要配置API接口的访问参数，如URL、认证信息等；
b) 阈值设置：针对不同的监控指标，设置合理的告警阈值。参考前面监控指标体系中设定的正常范围和告警阈值，在监控工具中进行相应的设置。例如，对于CPU使用率，可设置当使用率告警阈值为90%，即超过90%时触发告警；
c) 告警规则配置：定义告警的触发条件、告警方式和接收人等信息。例如，当CPU使用率超过90%且持续时间超过5分钟时，触发告警，通过邮件和短信的方式发送给系统管理员。

7 监控频率

7.1 不同指标和资源类型的监控频率确定

a) 关键性能指标：对于关键性能指标，如服务器的CPU使用率、内存使用率，虚拟机的CPU配额使用率、内存使用量等，应采用较高的监控频率。一般可设置为每分钟或每5分钟一次。这样可以及时捕捉到资源的使用变化情况，以便在出现问题时能够迅速采取措施；
b) 相对稳定的指标：对于一些相对稳定的指标，如存储设备的存储容量使用率、网络设备的带宽利用率等，可适当降低监控频率。例如，可设置为每小时或每天一次。因为这些指标在短期内变化不大，降低监控频率可以减少监控数据的存储量和分析工作量。

7.2 监控频率确定原则阐述

a) 资源的重要性：重要的资源，如核心服务器、关键存储设备等，应采用较高的监控频率，以确保其稳定运行。对于不太重要的资源，如一些边缘服务器或备用存储设备，可适当降低监控频率；
b) 业务需求：根据业务对资源的依赖程度和对性能的要求来确定监控频率。例如，对于实时性要求较高的业务，如在线交易系统，相关资源的监控频率应较高；对于一些非实时性业务，如数据备份系统，监控频率可适当降低；
c) 性能影响：考虑监控本身对资源性能的影响。过于频繁的监控可能会消耗一定的资源，如CPU时间、内存和网络带宽等。因此，在保证监控效果的前提下，应尽量选择合适的监控频率，以减少对资源性能的影响。

8 告警管理

8.1 告警阈值设置

8.1.1 设定方法和依据

a) 参考行业最佳实践：借鉴云计算行业内普遍认可的最佳实践经验，确定告警阈值。例如，在服务器CPU使用率方面，行业普遍认为当使用率超过90%时可能存在潜在风险，因此可将此作为告警阈值的参考；
b) 云计算平台的历史运行数据：分析云计算平台过去的运行数据，了解各项指标的正常波动范围和出现异常的情况。根据历史数据中的峰值和均值，结合当前业务需求，合理确定告警阈值。例如，如果历史数据显示服务器内存使用率在某些情况下会达到85%但仍能正常运行，那么可将告警阈值设定为90%；
c) 结合辽宁省的实际业务情况：考虑辽宁省本地的业务特点和需求，对告警阈值进行适当调整。例如，对于一些对温度敏感的业务，在监控服务器温度时，可能需要将告警阈值设置得比一般情况更低，以确保业务的正常运行。

8.1.2 动态调整机制

a) 根据业务变化进行调整：当业务发生变化，如业务量增加、业务类型改变等，相应的资源需求也会发生变化。此时，需要根据新的业务需求重新评估告警阈值。例如，当业务量增加导致服务器负载加重时，可能需要将CPU使用率的告警阈值适当降低，以更早地发现潜在问题；
b) 根据云计算平台的扩展进行调整：随着云计算平台的不断扩展，资源数量和配置也会发生变化。在这种情况下，需要根据新的资源配置和业务需求，重新设置告警阈值。例如，当增加了新的服务器或存储设备时，需要重新评估这些设备相关指标的告警阈值。

8.2 告警方式

8.2.1 支持的告警方式介绍

a) 邮件：通过邮件发送告警信息是一种常见的方式。在配置邮件告警时，需要设置发件人地址、收件人地址、邮件主题和内容格式等。邮件内容应包含告警的详细信息，如告警指标名称、当前值、告警阈值、发生时间等；
b) 短信：短信告警具有及时性强的特点。在配置短信告警时，需要设置短信发送平台的接入参数，如账号、密码、短信模板等。短信内容应简洁明了，突出告警的关键信息；
c) 系统弹窗：在监控系统的控制台或相关应用程序界面上弹出告警窗口，提醒运维人员注意。系统弹窗应显示告警的核心信息，如告警指标名称、当前值、告警阈值等。

8.2.2 确保告警信息准确性和及时性的措施

a) 数据验证：在发送告警信息之前，对采集到的数据进行验证，确保数据的准确性。例如，通过多次采集和对比，排除数据采集错误导致的误报；
b) 告警规则优化：不断优化告警规则，使其更加合理和准确。例如，对于一些容易出现波动的指标，可以设置一定的波动范围，在指标超出波动范围且持续一定时间后才触发告警，避免因指标的正常波动而频繁告警；
c) 实时监控系统性能：实时监控监控系统本身的性能，确保其能够及时处理和发送告警信息。如果监控系统出现故障或性能下降，可能会导致告警信息延迟或丢失。

8.3 告警处理流程

8.3.1 定义告警的接收、确认、处理和反馈流程

a) 接收：运维人员通过邮件、短信或系统弹窗等方式接收告警信息。在接收告警信息后，应立即查看告警的详细内容，了解告警的原因和相关指标的情况；
b) 确认：对告警信息进行确认，判断告警是否真实有效。如果是误报，需要记录误报原因并对告警系统进行相应调整；如果告警属实，则进入处理阶段；
c) 处理：根据告警的类型和相关指标的情况，采取相应的处理措施。例如，如果是服务器CPU使用率过高的告警，需要检查运行的程序，看是否有异常进程占用大量CPU资源，必要时可以终止相关进程或对服务器进行资源调整。处理过程中应详细记录处理步骤和结果；
d) 反馈：在处理完告警后，将处理结果反馈给相关人员，如上级主管或其他相关部门。反馈内容应包括告警的原因、处理措施和最终结果，以便相关人员了解情况，并对云计算平台的运行维护进行评估和改进。

8.3.2 明确告警处理各环节的责任人和时间要求

a) 接收责任人：运维值班人员为告警接收的第一责任人，应在告警发出后的5分钟内查看告警信息；
b) 确认责任人：由经验丰富的运维工程师负责告警确认，应在接收告警后的10分钟内完成确认工作；
c) 处理责任人：根据告警的具体内容确定处理责任人，如系统管理员负责服务器相关告警的处理，存储工程师负责存储设备相关告警的处理等。处理责任人应在确认告警后的30分钟内开始处理，并尽快完成处理工作，一般要求在2小时内解决问题（对于复杂问题可适当延长处理时间，但需及时向上级汇报进展情况）；
d) 反馈责任人：处理责任人在处理完告警后应及时将反馈信息发送给相关人员，一般要求在处理完成后的10分钟内完成反馈。

9 监控数据分析与报告

9.1 数据分析方法

9.1.1 统计分析

a) 描述统计量计算：计算监控指标的均值、中位数、标准差等描述统计量，以了解指标的集中趋势和离散程度。例如，通过计算服务器CPU使用率的均值和标准差，可以判断服务器的负载是否稳定，标准差过大可能表示负载波动较大；
b) 相关性分析：分析不同监控指标之间的相关性，以发现潜在的问题和关系。例如，分析服务器CPU使用率和内存使用率之间的相关性，如果两者高度相关，可能表示存在内存泄漏或程序对资源的不合理使用。

9.1.2 趋势分析

a) 时间序列分析：对监控指标随时间的变化进行分析，绘制时间序列图，观察指标的变化趋势。例如，通过观察存储容量使用率的时间序列图，可以预测存储设备何时需要扩容；
b) 移动平均分析：采用移动平均法对监控指标进行平滑处理，去除短期波动，更好地观察指标的长期趋势。例如，对网络带宽利用率进行移动平均分析，可以更清晰地看到网络负载的长期变化情况。

9.1.3 通过数据分析发现问题和风险的示例

a) 资源瓶颈发现：通过对服务器CPU使用率和内存使用率的分析，如果发现两者同时接近或超过告警阈值，且持续时间较长，可能表示服务器存在资源瓶颈，需要对服务器进行升级或优化资源分配；
b) 性能异常发现：分析某一时间段内虚拟机的虚拟磁盘读写速率，如果发现读写速率突然下降且低于正常范围，可能表示虚拟机内部的存储系统出现故障，需要进一步检查虚拟机的配置和存储设备的连接情况。

9.2 监控报告生成

9.2.1 报告内容和格式规定

a) 监控指标的统计数据：包括各个监控指标的均值、最大值、最小值、标准差等统计数据，以及统计数据所对应的时间段。例如，报告中应列出服务器CPU使用率在过去一天内的均值为60%，最大值为85%，最小值为35%，标准差为10%；
b) 趋势图表：包含各个监控指标的时间序列图、移动平均图等趋势图表，以直观地展示指标的变化趋势。例如，绘制服务器CPU使用率的时间序列图，展示过去一周内CPU使用率的变化情况；
c) 告警情况汇总：总结报告期内发生的所有告警事件，包括告警指标名称、告警次数、告警阈值、实际值、处理情况等。例如，报告中说明在过去一天内服务器CPU使用率告警3次，告警阈值为90%，实际值分别为92%、93%、94%，处理情况为已通过终止异常进程解决问题。

9.2.2 报告生成周期和发送对象明确

a) 生成周期：监控报告分为日报告、周报告和月报告。日报告应在每天工作结束后生成，周报告在每周周末生成，月报告在每月月末生成；

b) 发送对象：日报告发送给运维团队的所有成员，以便他们及时了解当天的云计算平台运行情况；周报告发送给运维团队负责人和相关业务部门负责人，用于对本周的运行维护情况进行总结和评估；月报告发送给公司高层管理人员、运维团队负责人和相关业务部门负责人，以便他们对整个月的云计算平台运行情况有一个全面的了解，并为决策提供依据。

10 安全与隐私保护

10.1 监控数据安全

10.1.1 采集过程中的安全措施

a) 加密传输：在数据采集过程中，对采集到的数据进行加密传输，防止数据在传输过程中被窃取或篡改。例如，采用SSL/TLS协议对基于代理采集的数据进行加密传输，确保数据的安全性；
b) 身份认证：建立身份认证机制，确保只有授权的采集设备或工具才能进行数据采集。例如，在代理软件中设置用户名和密码，只有输入正确的用户名和密码才能启动采集程序。

10.1.2 传输过程中的安全措施

a) 安全协议应用：在数据传输过程中，继续使用安全协议如SSL/TLS确保数据的安全性。同时，对传输的数据包进行完整性检查，防止数据在传输过程中被篡改；
b) 网络隔离：根据需要，对监控数据传输的网络进行隔离，避免监控数据与其他业务数据混合传输，降低数据泄露的风险。

10.1.3 存储过程中的安全措施

a) 加密存储：对存储的监控数据进行加密存储，防止数据在存储过程中被窃取或篡改。例如，采用AES等加密算法对数据进行加密，只有拥有正确解密密钥的人员才能访问数据；
b) 访问控制：建立严格的访问控制机制，限制只有授权人员才能访问监控数据。通过设置用户角色和权限，明确不同人员对监控数据的访问权限，如运维人员可以查看和分析数据，而普通员工则无法访问。

10.1.4 处理过程中的安全措施

a) 安全的数据分析工具：使用安全的数据分析工具对监控数据进行处理，避免因工具本身的漏洞导致数据泄露或篡改。例如，选择经过安全认证的数据分析软件，定期更新软件版本以修复已知漏洞；
b) 操作审计：对监控数据的处理过程进行操作审计，记录每一个操作步骤和操作人员，以便在出现问题时能够进行追溯。

10.2 隐私保护

10.2.1 明确隐私范畴的数据

a) 用户身份信息：包括用户名、密码、用户ID等用户身份识别信息，在监控过程中应避免收集和处理这些信息，除非有明确的法律授权或用户同意；
b) 用户业务数据：用户在云计算平台上存储和处理的业务数据，如文件内容、数据库记录等，这些数据的监控应严格按照隐私政策和相关法律法规进行，确保不侵犯用户的隐私权。

10.2.2 保护措施

a) 数据脱敏：对于可能涉及隐私的监控数据，如用户访问的IP地址等，进行数据脱敏处理，将真实数据替换为虚拟数据或进行模糊处理，使数据无法直接识别用户身份；
b) 隐私政策遵守：制定和遵守严格的隐私政策，明确在监控过程中如何保护用户隐私，并向用户公示隐私政策，取得用户的信任。

11 实施与监督

11.1 实施步骤

11.1.1 前期准备

a) 需求分析：对云计算平台的运行维护需求进行分析，确定需要监控的资源类型和监控指标。例如，根据业务需求和平台架构，确定需要对服务器的CPU、内存、磁盘和网络等资源进行监控，并明确相应的监控指标；
b) 工具选型：根据需求分析的结果，选择适合的监控工具和方法。参考前面监控工具选择与配置部分的内容，选择开源工具如Zabbix或商业软件如SolarWinds，并确定相应的采集方法，如基于代理采集或无代理采集；
c) 人员培训：对参与云资源监控实施的人员进行培训，包括监控工具的使用方法、监控指标的含义、告警处理流程等内容。培训可以通过内部培训课程、在线学习平台或邀请专家授课等方式进行。

11.1.2 监控系统部署

a) 硬件环境准备：根据监控工具的要求，准备好相应的硬件环境。例如，如果选择的监控工具需要安装在服务器上，需要准备一台或多台服务器，并确保服务器具备足够的计算能力、内存和存储容量；
b) 软件环境准备：安装和配置监控工具所需的软件环境。例如，安装操作系统、数据库管理系统、监控工具本身及其依赖的软件库等；
c) 代理软件部署（如果适用）：如果选择基于代理的采集方法，在需要监控的设备上部署代理软件，并进行相应的配置。

11.1.3 指标配置

a) 监控指标设置：在监控工具中设置需要监控的指标，根据前面监控指标体系部分的内容，设置各个指标的正常范围、告警阈值等参数；
b) 告警规则设置：设置告警规则，包括告警的触发条件、告警方式和接收人等信息。例如，设置当服务器CPU使用率超过90%且持续时间超过5分钟时，触发告警，通过邮件和短信的方式发送给系统管理员。

11.1.4 测试验证

a) 功能测试：对监控系统进行功能测试，检查监控系统是否能够正常采集数据、分析数据和触发告警。例如，通过模拟不同的资源使用情况，检查监控系统是否能够准确采集CPU使用率、内存使用率等指标，并在指标超过告警阈值时触发告警；
b) 性能测试：对监控系统进行性能测试，检查监控系统是否会对云计算平台的资源造成过大的影响。例如，在监控系统运行的同时，观察其服务器的CPU使用率、内存使用率等指标是否有明显变化，如果变化过大，可能需要对监控系统进行优化。

11.2 监督与检查

11.2.1 监督机制建立

a) 部门职责明确：明确相关部门或机构在云计算平台云资源监控实施情况监督中的职责。例如，由信息安全部门负责监督监控数据的安全和隐私保护情况，由运维管理部门负责监督监控系统的运行效果和告警处理情况；
b) 检查内容确定：确定监督检查的内容，包括监控指标的设置是否合理、告警阈值是否正确、监控频率是否合适、监控工具是否正常运行、监控数据是否安全等。

11.2.2 定期检查和不定期抽查方式和频率规定

a) 定期检查：定期对云计算平台的云资源监控实施情况进行检查，例如每月进行一次全面检查。检查内容包括上述确定的各项内容，通过查看监控报告、检查监控系统配置等方式进行；
b) 不定期抽查：不定期对云计算平台的云资源监控实施情况进行抽查，例如每周随机抽取部分设备或指标进行检查。抽查内容主要针对重点设备、关键指标和容易出现问题的地方，如服务器的CPU使用率、存储设备的存储容量使用率等。

11.3 问题整改

a) 整改要求制定：对于监督检查中发现的不符合本文件要求的情况，制定相应的整改要求。例如，如果发现监控指标设置不合理，要求重新设置监控指标，明确合理的正常范围和告警阈值；如果发现监控频率设置不合理，要求调整监控频率，使其符合本文件的要求；
b) 期限规定：给整改单位或人员规定整改期限，一般要求在10天内完成整改（对于复杂问题可适当延长整改时间，但需向上级汇报进展情况）；
c) 复查方式确定：确定复查方式，在整改期限结束后，通过再次检查监控系统配置、查看监控报告等方式对整改情况进行复查，确保整改措施有效，符合本文件的要求。