

团 体 标 准

T/NDAS XX—2020

基于大数据的云服务保护技术

Cloud service protection technology based on big data

（征求意见稿）

XXXX—XX—XX 发布

XXXX—XX—XX 实施

宁德市标准化协会 发布

目 次

前 言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 云服务保障管理体系结构..... 2

5 云服务保障管理流程定义方法..... 2

6 监控管理..... 2

 6.1 角色..... 2

 6.2 职责..... 3

 6.3 指标..... 3

 6.4 流程..... 3

7 事故管理..... 5

 7.1 角色..... 5

 7.2 职责..... 5

 7.3 指标..... 6

 7.4 流程..... 6

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 提出。

本文件由宁德市标准化协会归口。

本文件起草单位：

本文件主要起草人：

基于大数据的云服务保护技术

1 范围

本文件规定了基于大数据的云服务保护技术的体系结构、管理流程定义方法、监控管理及事故管理。本文件适用于开展云服务保障管理活动所需的人员及流程设计、运营支撑系统建设、运维质量评价等。

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。

YD/T 1926.1 IT运维服务管理技术要求 第1部分：体系架构

YD/T 1926.3 IT运维服务管理技术要求 第3部分：服务管理流程

3 术语和定义

YD/T 1926.1和YD/T 1926.3中界定的以及下列术语和定义适用于本文件。

3.1

服务等级协议 service level agreement

服务提供商和客户签订的书面协议，该协议中明确规定了服务和规定的服务等级。

3.2

事件 incident

对配置项或云服务管理有意义的状态变化以及来自客户的请求。

3.3

事故 accident

导致或可能导致云保障管理不在计划范围内的中断或质量下降的事件。

3.4

问题 question

一个或多个事故的未知的根本原因。

3.5

客户 client

云保障管理服务的购买者，与服务提供商定义和协商服务的内容和质量要求，并为服务支付费用。

4 云服务保障管理体系结构

云服务保障管理体系结构如图1所示。

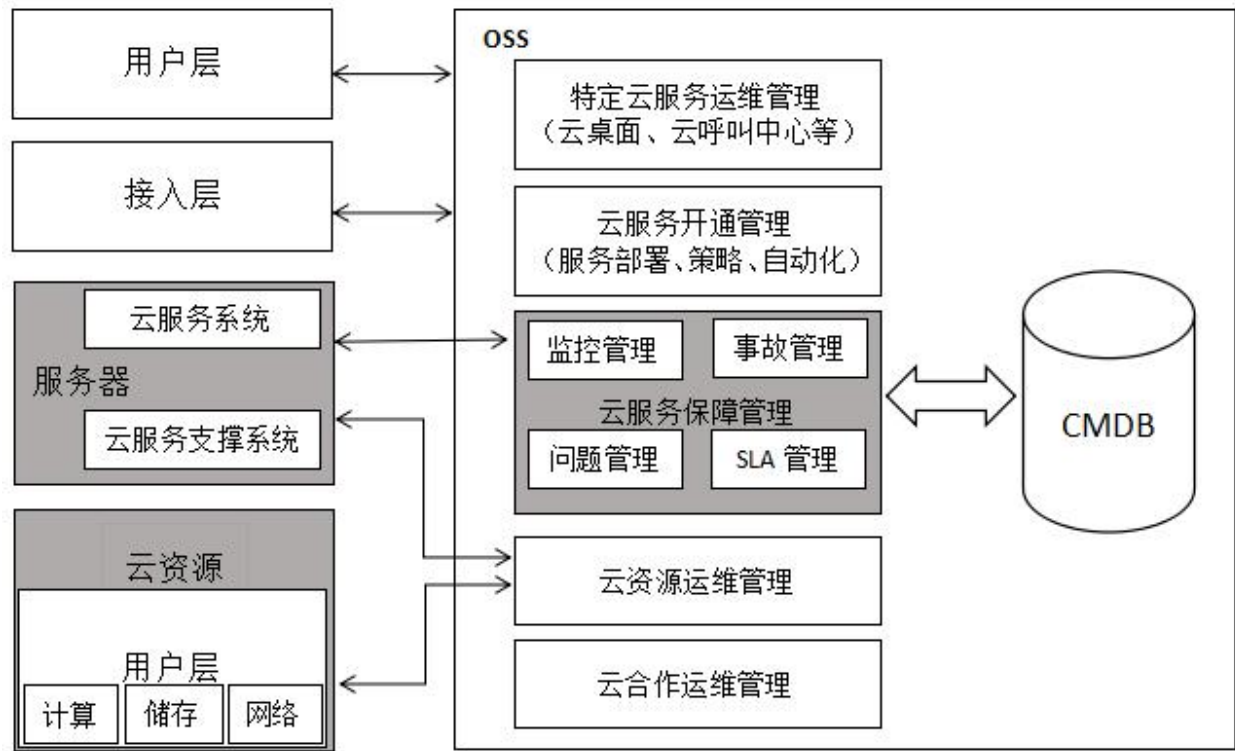


图 1 云服务保障管理体系结构

5 云服务保障管理流程定义方法

云服务保障管理从运维角色、职责、流程、指标等方面进行定义，其中：

- a) 角色：指被赋予一组职责的个人或团队；
- b) 职责：包括责任、活动以及权利等；
- c) 流程：包括流程图和流程说明；
- d) 指标：用于衡量角色或流程的效率。

6 监控管理

6.1 角色

6.1.1 服务台

服务台既是连接云保障管理服务提供商和客户的桥梁，也是接收云资源运维管理系统告警信息及接口，主要服务管理事件和服务请求，也负责与客户保持必要的联系。

6.1.2 事件管理者

事件管理者该角色由一人或多人担任，负责对提交自服务台的事件进行管理，包括对事件的分类、转发等。

6.2 职责

6.2.1 服务台职责

服务台的职责主要包括以下内容：

- a) 接收来自客户的请求事件；
- b) 接收来自云资源运维管理系统的事件信息；
- c) 接收来自云服务系统的时间信息；
- d) 记录并跟踪事件和客户意见；
- e) 与客户沟通，既是通知他们请求的当前进展状况。

6.2.2 事件管理者职责

事件管理者的职责主要包括以下内容：

- a) 将来自服务台的事件信息进行过滤、分类、并将事件提交到不同的处理流程；
- b) 当事件被认定为问题后，事件管理人员将事件转交到问题管理者，启动问题管理流程；
- c) 当事件被认定为事故后，事件管理人员需要对其进行必要的调查，并将结果与事故一起提交给事故管理者，启动事故管理流程；
- d) 当事件处理完毕或被提交到其它流程后，事件管理者需关闭事件并根据事件处理更新知识库。

6.3 指标

为了更好的控制监控管理的流程，需要为其设置度量指标，监控管理的关键度量指标包括：

- a) 各类事件的数量 5；
- b) 可自动响应的事件的 50 %；
- c) 要求人为干预的事件的 30 %；
- d) 重复发生的事件的 3 %；
- e) 标志着某种性能问题的事件的 1 %；
- f) 标志着潜在的可用性问题的事件的 1 %。

6.4 流程

6.4.1 流程图

监控管理流程如图2所示。

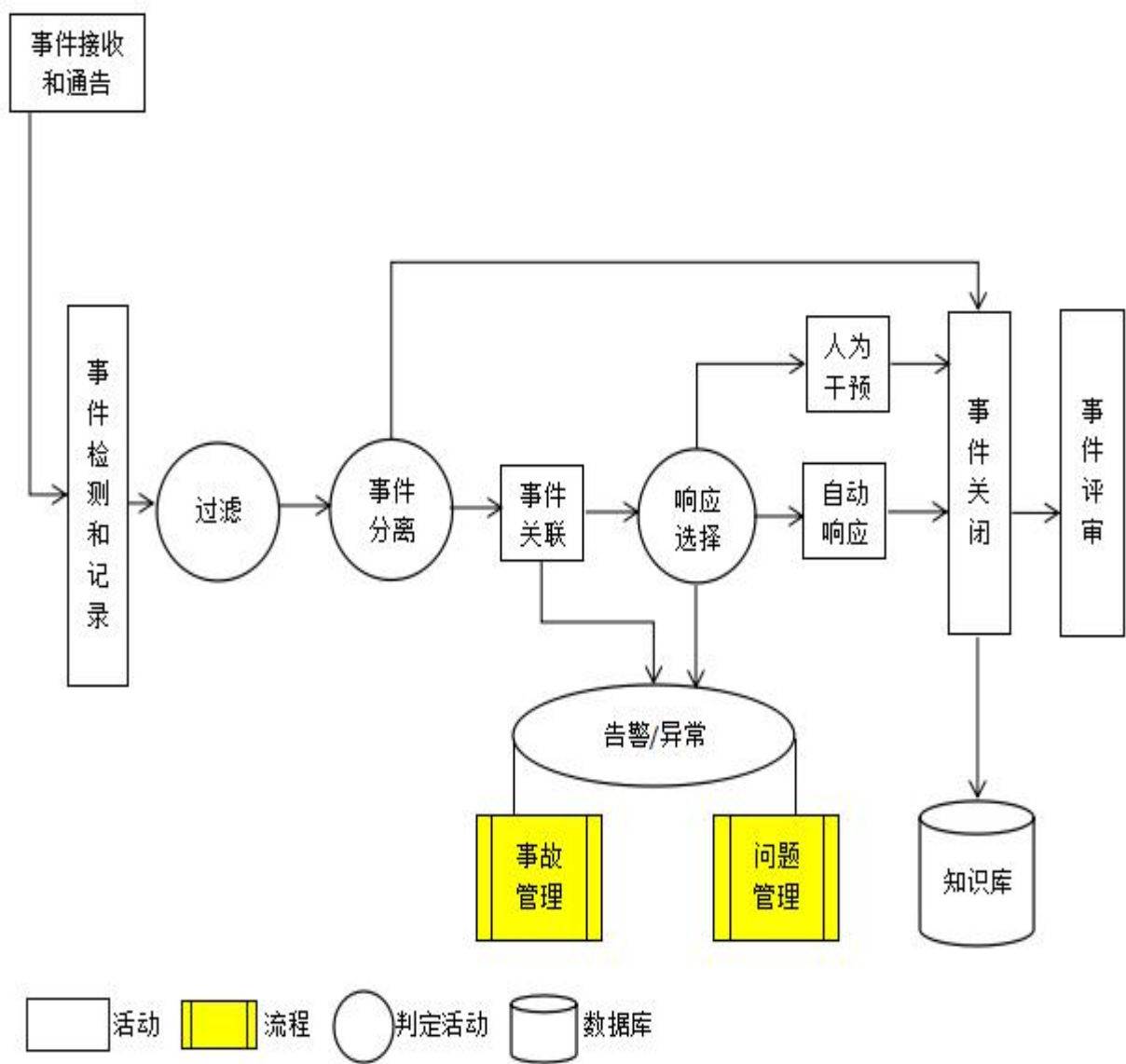


图 2 监控管理流程

6.4.2 流程说明

监控管理流程说明如表1所示。

表 1 监控管理流程说明

序号	步骤名称	责任人	说明
1	事件的接收和通告	服务台	1、接收来自客户的请求事件、云资源运维管理系统及云服务系统的告警信息； 2、接收事件后，通过轮询或通知的方式生产通告信息发给事件管理者。
2	事件监测和记录	事件管理者	1、通过管理工具检测和解析通告信息； 2、将检测到的事件信息录入事件操作日志。

表 1（续）监控管理流程说明

序号	步骤名称	责任人	说明
3	事件过滤	事件管理者	1、对检测出的事件进行必要的过滤，以确定哪些事件应被忽略； 2、对于过滤掉的事件应当及时记录到日志文件中。
4	事件分类判定	事件管理者	1、对过滤后的事件按照其重要性进行必要的分类，类型包括信息类、告警类以及异常类； 2、信息类事件直接结束； 3、告警类事件进行事件关联分析； 4、异常类事件进行进一步升级，启动事故，问题管理中的必要流程来处理。
5	事件关联	事件管理者	1、通过特定的管理工具将告警类事件与一组事先规定的标准和规则进行比较，从而识别事件的意义并确定相应的事件处理行动。
6	响应选择	事件管理者	1、依据事件关联的分析结果，触发相应的处理方式。

7 事故管理

7.1 角色

7.1.1 事故管理者

事故管理者负责在事故管理流程中协调和监控事故的解决。

7.1.2 一线支持人员

一线支持人员比事故管理者具有更多的专业技能，负责进一步解决提交事故。

7.1.3 事故处理专家

事故处理专家由内部的专家、厂商专家及供应商组成。

7.2 职责

7.2.1 事故管理者的职责

事故管理者的职责包括以下内容：

- a) 监控事故处理流程的效率和效果；
- b) 分派、管理事故支持小组的工作；
- c) 协调各方资源以确保方案的成功制定和实施；
- d) 管理重大事故。

7.2.2 一线支持人员的职责

一线支持人员的职责包括以下内容：

- a) 接收提交自事件监控流程、云服务系统及云资源运维管理系统的事故信息，并对其性质进行判断，将不属于事故的事件转交到问题管理等其它流程处理；
- b) 对记录的事故进行分类及优先级判定；
- c) 验证事故的描述和信息，进一步收集相关信息；
- d) 实施事故解决方案，更新事故解决信息。

7.2.3 事故处理专家的职责

事故处理专家的职责包括以下内容：

- a) 必要时提供现场支持和深入调查和研究，提供有效的解决方案；
- b) 提供设备相关信息，参与解决方案的实施。

7.3 指标

为了较好的控制事故管理的质量，需要为其设置度量指标，事故管理的关键度量指标包括：

- a) 事故总数；
- b) 当前积压的事故；
- c) 重大事故的数量；
- d) 平均解决时间；
- e) 每个事故的平均成本；
- f) 被错误分配的事故的数量和百分比；
- g) 正确转交的事故数量和百分比；
- h) 无需拜访客户而远程解决事故数量和百分比。

7.4 流程

7.4.1 事故管理流程图

事故管理流程图如图3所示。

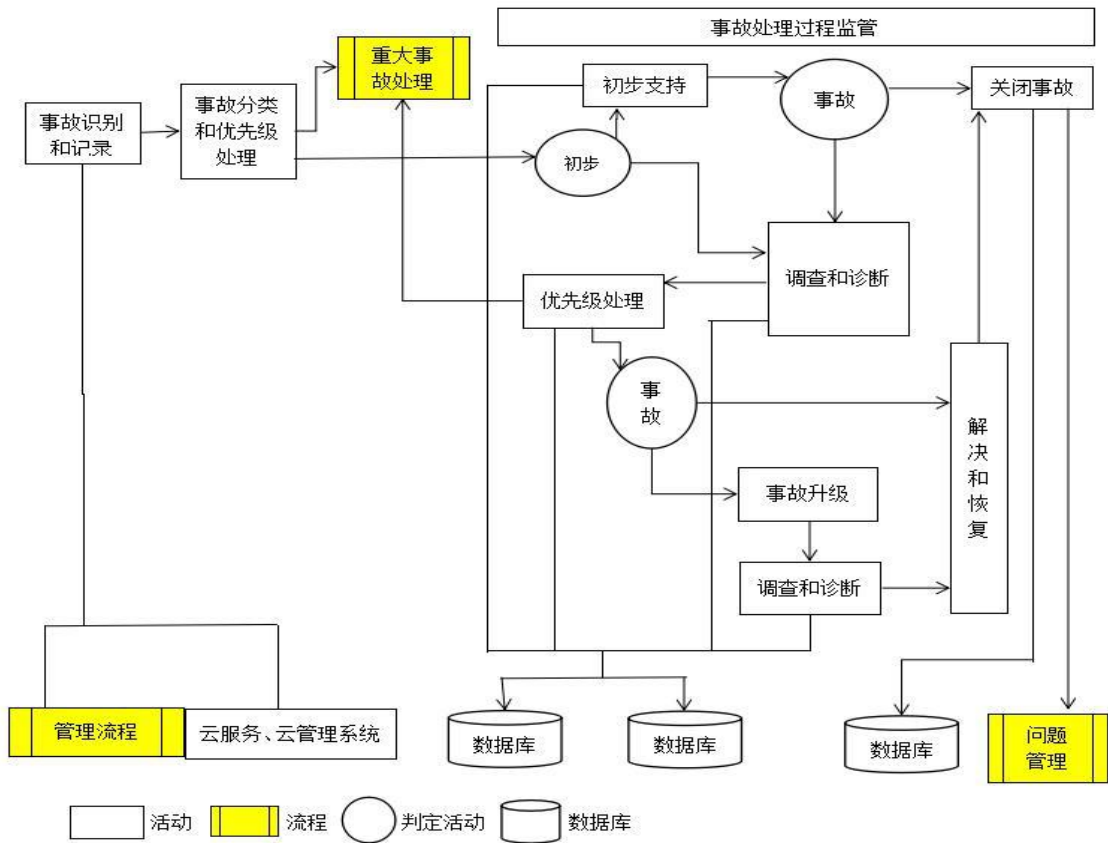


图 3 事故管理流程

7.4.2 流程说明

事故管理流程说明如表2所示。

表 2 事故管理流程说明

序号	步骤名称	责任人	说明	关联流程
1	事故识别和记录	一线支持人员	a) 一线支持人员对来自监控管理的事故进行详细记录，主要包括来自云服务基础设施的故障告警、来自客服和业务部门的客户投诉等； b) 一线支持人员需把不属于事故的事件转交到其它流程予以处理。	监控管理
2	事故分类和优先级处理	一线支持人员	a) 一线支持人员对记录的事故进行分类； b) 一线支持人员对记录的事故进行优先级处理，定义出事故的影响度和紧急度； c) 当支持人员根据服务等级管理提供的服务级别协议判定事故的影响度和紧急度达到重大事故标准时，则转交重大事故处理流程。	