



(12) 发明专利

(10) 授权公告号 CN 112559237 B

(45) 授权公告日 2021.07.06

(21) 申请号 202110188400.X

审查员 姚子琪

(22) 申请日 2021.02.19

(65) 同一申请的已公布的文献号

申请公布号 CN 112559237 A

(43) 申请公布日 2021.03.26

(73) 专利权人 北京必示科技有限公司

地址 100083 北京市海淀区中关村东路8号

东升大厦B座516

(72) 发明人 汤汝鸣 隋楷心 刘大鹏

(74) 专利代理机构 北京华创智道知识产权代理

事务所(普通合伙) 11888

代理人 彭随丽

(51) Int. Cl.

G06F 11/07 (2006.01)

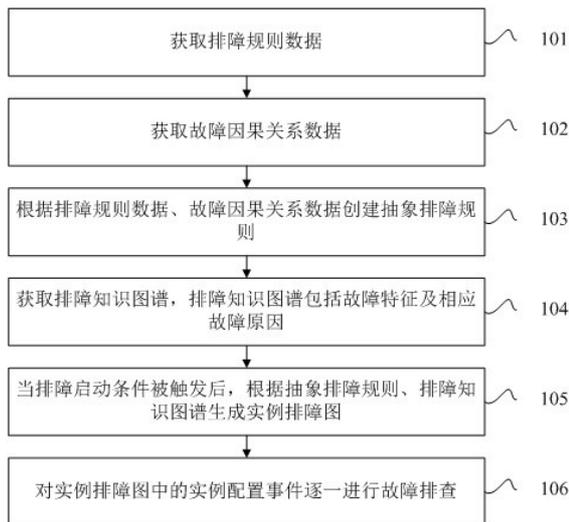
权利要求书2页 说明书13页 附图9页

(54) 发明名称

运维系统排障方法、装置、服务器和存储介质

(57) 摘要

本发明实施例涉及运维系统排障技术领域，公开了一种运维系统排障方法、装置、服务器和存储介质。该方法根据排障规则数据、故障因果关系数据创建抽象排障规则，抽象排障规则包括抽象配置事件和抽象配置规则，抽象配置事件表示虚拟排障对象，抽象配置规则表示虚拟配置事件之间的关系；当排障启动条件被触发后，根据抽象排障规则、排障知识图谱生成实例排障图，实例排障图包实例化的虚拟事件和实例化的抽象配置规则，对实例排障图中的实例配置事件逐一进行故障排查，本发明通过建立通用排障规则，在具体业务场景，对不同的运维实体对象进行抽象，通过学习专家的运维经验，将运维经验抽象成排障图，由排障引擎自动执行，完成运维系统排障工作。



1. 一种运维系统排障方法,其特征在于,包括:获取排障规则数据;获取故障因果关系数据;根据所述排障规则数据、所述故障因果关系数据创建抽象排障规则,所述抽象排障规则包括抽象配置事件和抽象配置规则,所述抽象配置事件表示虚拟排障对象,所述抽象配置规则表示抽象配置事件之间的关系;获取排障知识图谱,所述排障知识图谱包括故障特征及相应故障原因;当排障启动条件被触发后,根据所述抽象排障规则、所述排障知识图谱生成实例排障图,所述实例排障图包括实例配置事件和实例配置规则,所述实例配置事件是实例化的所述抽象配置事件,所述实例配置规则是实例化的所述抽象配置规则;对所述实例排障图中的实例配置事件逐一进行故障排查;

其中,排障规则数据由人工输入;

在所述排障启动条件被触发前,所述方法还包括:获取异常检测数据;所述根据所述抽象排障规则、所述排障知识图谱生成实例排障图:根据所述抽象排障规则、所述排障知识图谱和所述异常检测数据生成实例排障图;

所述排障启动条件包括以下方式中的一种或多种:方式一、其他监控和/或告警平台的API触发;方式二、流式数据阈值触发;方式三、流式数据异常检测触发;方式四、其他脚本命令触发;

还包括:对排查出的故障信息进行根因定位,以确定故障产生的原因;

所述抽象排障规则和所述实例排障图是包括节点和边的树状图,所述抽象配置事件和所述实例配置事件与节点对应,所述抽象配置规则和所述实例配置规则与边对应,所述根据所述抽象排障规则、所述排障知识图谱生成实例排障图包括:对于每个包含子结点的节点,给每个子节点赋值一个实体对象,所述实体对象由相应的根结点或父结点确定;

所述根据所述抽象排障规则、所述排障知识图谱生成实例排障图还包括:根据所述抽象排障规则中边的类型确定子结点的实体对象;

所述排障知识图谱还包括实体的空间关系,所述根据所述抽象排障规则图中边的类型确定子结点的实体对象包括:若边的类型为“同对象”,则子结点直接继承父结点的实体对象;若边的类型不是“同对象”,则调用相应的空间关系数据,根据父结点、子结点各自的空间类型,查找对应的实体对象;

所述抽象配置事件和实例配置事件包括基本事件和虚拟事件,所述基本事件为真实事件,所述虚拟事件为概念事件,每个所述虚拟事件链接至少一个基本事件,所述虚拟事件链接的任一个所述基本事件,只要有一个基本事件结点异常则相应虚拟事件结点异常;

所述基本事件包含检测实体、检测数据、检测方法和可视化面板;

所述检测实体抽象成类型,根据需求定义生效范围,与所述排障知识图谱管理解耦;和/或,所述检测数据抽象成类型或者接口,根据需求定义生效范围,与指标对象管理解耦;和/或,所述检测方法为规则、算法或查询脚本,与检测逻辑解耦。

2. 根据权利要求1所述的运维系统排障方法,其特征在于,还包括:图形化显示所述抽象排障规则,和/或,图形化显示所述实例排障图。

3. 根据权利要求1所述的运维系统排障方法,其特征在于,所述抽象配置规则包括相应抽象配置事件的原因事件、结果事件、空间关系、时间关系和权重五部分。

4. 根据权利要求1所述的运维系统排障方法,其特征在于,所述基本事件为指定对象,或所述基本事件为指定类型对象。

5. 根据权利要求1所述的运维系统排障方法,其特征在于,所述虚拟事件链接的基本事件之间为或的关系。

6. 一种运维系统排障装置,用于实现如权利要求1至5中任一所述的运维系统排障方法,其特征在于,包括:规则数据获取模块,用于获取排障规则数据;因果关系获取模块,用于获取故障因果关系数据;抽象规则创建模块,用于根据所述排障规则数据、所述故障因果关系数据创建抽象排障规则,所述抽象排障规则包括抽象配置事件和抽象配置规则,所述抽象配置事件表示虚拟排障对象,所述抽象配置规则表示所述抽象配置事件之间的关系;图谱获取模块,用于获取排障知识图谱,所述排障知识图谱包括故障特征及相应故障原因;实例排障图创建模块,用于当排障启动条件被触发后,根据所述抽象排障规则、所述排障知识图谱生成实例排障图,所述实例排障图包括实例配置事件和实例配置规则,所述实例配置事件是实例化的所述抽象配置事件,所述实例配置规则是实例化的所述抽象配置规则;故障排查模块,用于对所述实例排障图中的实例配置事件逐一进行故障排查。

7. 一种服务器,其特征在于,包括:至少一个处理器;以及,与所述至少一个处理器通信连接的存储器;其中,所述存储器存储有被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行如权利要求1至5中任一所述的运维系统排障方法。

8. 一种计算机可读存储介质,存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现权利要求1至5中任一项所述的运维系统排障方法。

运维系统排障方法、装置、服务器和存储介质

技术领域

[0001] 本发明实施例涉及运维系统排障技术领域,特别涉及运维系统排障方法、装置、服务器和存储介质。

背景技术

[0002] 在大型企业,尤其是银行、证券等公司的数据中心、生产网络中,运行着数量庞大的各类业务系统(简称为系统),而各个系统本身、系统之间的数据吞吐量也十分巨大。在这些网络中,各种系统复杂而庞大,同时,各个系统组件之间的关联关系也极其复杂,这对于整个系统的运维工作提出了巨大的挑战。为了有效监控、排查复杂网络条件中的各种故障,在大型的生产网络中,建立了许多不同的网络、设备的监控设施和平台,对系统及其关联的网络设备、物理组件等关键指标进行监控和告警,这些告警、错误日志、监控指标等构成了业务排障的基础。

[0003] 在一个复杂的生产网络中,故障的影响范围往往不会局限于单一的设备。一般当业务系统发生故障时,故障会级联触发多个其他的系统异常,例如某个业务系统的交易量发生了明显下降,这既有可能是由于该业务系统本身的设备故障导致的,也有可能是其下游应用或子系统的故障导致的。这一现象导致在实际处理中,运维人员往往需要排查更广的范围才能准确判断故障发生的原因。另一方面,在实际的大型企业的内部网络环境中,不同的业务系统、设备可能归属于不同的运维处室、小组,其数据可能存在于不同的监控平台。为准确排查故障原因,运维人员需要协调不同部门的人员,将这些散落在不同的地方的数据、信息进行统一的收集、汇总、处理,需要很高的沟通成本,效率低下。最后,传统的方法是通过人工逐个排查,手动做信息汇总,让运维专家来决定如何止损和找到故障根本原因,整个过程耗时长。同时专家排障经验都在人脑中,很难做到积累并传承。

[0004] 总结来说,发明人发现传统的排障流程至少存在如下问题:

[0005] 1) 故障涉及多个系统异常,排障范围广、难度高;

[0006] 2) 多方协作排障,信息收集慢,人工排障时间长;

[0007] 3) 专家积累大量故障分析决策经验,难以沉淀固化、重复利用。

发明内容

[0008] 为有效解决背景技术中的至少一个问题,本发明实施方式的目的在于提供一种运维系统排障方法、装置、服务器和存储介质,建立通用排障规则,在具体业务场景,对不同的运维实体对象进行抽象,通过学习专家的运维经验,将运维经验抽象成排障图,由排障引擎自动执行,完成运维系统排障工作。

[0009] 为解决上述技术问题,一方面的本发明的实施方式提供了一种运维系统排障方法,包括:

[0010] 获取排障规则数据;

[0011] 获取故障因果关系数据;

[0012] 根据所述排障规则数据、所述故障因果关系数据创建抽象排障规则,所述抽象排障规则包括抽象配置事件和抽象配置规则,所述抽象配置事件表示虚拟排障对象,所述抽象配置规则表示所述虚拟配置事件之间的关系;

[0013] 获取排障知识图谱,所述排障知识图谱包括故障特征及相应故障原因;

[0014] 当排障启动条件被触发后,根据所述抽象排障规则、所述排障知识图谱生成实例排障图,所述实例排障图包括实例配置事件和实例配置规则,所述实例配置事件是实例化的所述虚拟事件,所述实例配置规则是实例化的所述抽象配置规则;

[0015] 对所述实例排障图中的实例配置事件逐一进行故障排查。

[0016] 进一步可选的,在所述排障启动条件被触发前,所述方法还包括:

[0017] 获取异常检测数据;

[0018] 所述根据所述抽象排障规则、所述排障知识图谱生成实例排障图:根据所述抽象排障规则、所述排障知识图谱和所述异常检测数据生成实例排障图。

[0019] 进一步可选的,所述排障启动条件包括以下方式中的一种或多种:

[0020] 方式一、其他监控和/或告警平台的API触发;

[0021] 方式二、流式数据阈值触发;

[0022] 方式三、流式数据异常检测触发;

[0023] 方式四、其他脚本命令触发。

[0024] 进一步可选的,还包括:

[0025] 对排查出的故障信息进行根因定位,以确定故障产生的原因。

[0026] 进一步可选的,所述抽象排障规则和所述实例排障图是包括节点和边的树状图,所述抽象配置事件和所述实例配置事件与节点对应,所述抽象配置规则和所述实例配置规则与边对应,所述根据所述抽象排障规则、所述排障知识图谱生成实例排障图包括:

[0027] 对于每个包含子结点的节点,给每个子节点赋值一个实体对象,所述实体对象由相应的根结点或父结点确定。

[0028] 进一步可选的,所述根据所述抽象排障规则、所述排障知识图谱生成实例排障图还包括:

[0029] 根据所述抽象排障规则图中边的类型确定子结点的实体对象。

[0030] 进一步可选的,所述Oracle排障知识图谱还包括实体的空间关系,所述根据所述抽象排障规则图中边的类型确定子结点的实体对象包括:

[0031] 若边的类型为“同对象”,则子结点直接继承父结点的实体对象;和/或,

[0032] 若边的类型不是“同对象”,则调用相应的空间关系数据,根据父结点、子结点各自的空间类型,查找对应的实体对象。

[0033] 进一步可选的,还包括:

[0034] 图形化显示所述抽象排障规则,和/或,图形化显示所述实例排障图。

[0035] 进一步可选的,所述抽象配置事件和实例配置事件包括基本事件和虚拟事件,所述基本事件为真实事件,所述虚拟事件为概念事件,每个所述虚拟事件链接至少一个基本事件,所述虚拟事件链接的任一个所述基本事件,只要有一个基本事件结点异常则相应虚拟事件结点异常。

[0036] 进一步可选的,所述基本事件包含检测实体、检测数据、检测方法和可视化面板。

- [0037] 进一步可选的,所述检测实体抽象成类型,根据需求定义生效范围,与所述排障知识图谱CMDB管理解耦;和/或,
- [0038] 所述检测数据抽象成类型或者接口,根据需求定义生效范围,与指标对象管理解耦;和/或,
- [0039] 所述测方法为规则、算法或查询脚本,与检测逻辑解耦。
- [0040] 进一步可选的,所述抽象配置规则包括相应抽象配置事件的原因事件、结果事件、空间关系、时间关系和权重五部分。
- [0041] 进一步可选的,所述基本事件为指定对象,或所述基本事件为指定类型对象。
- [0042] 进一步可选的,所述虚拟事件链接的基本事件之间为或的关系。
- [0043] 另一方面,一种运维系统排障装置,包括:
- [0044] 规则数据获取模块,用于获取排障规则数据;
- [0045] 因果关系获取模块,用于获取故障因果关系数据;
- [0046] 抽象规则创建模块,用于根据所述排障规则数据、所述故障因果关系数据创建抽象排障规则,所述抽象排障规则包括抽象配置事件和抽象配置规则,所述抽象配置事件表示虚拟排障对象,所述抽象配置规则表示所述虚拟配置事件之间的关系;
- [0047] 图谱获取模块,用于获取排障知识图谱,所述排障知识图谱包括故障特征及相应故障原因;
- [0048] 实例排障图创建模块,用于当排障启动条件被触发后,根据所述抽象排障规则、所述排障知识图谱生成实例排障图,所述实例排障图包括实例配置事件和实例配置规则,所述实例配置事件是实例化的所述虚拟事件,所述实例配置规则是实例化的所述抽象配置规则;
- [0049] 故障排查模块,用于对所述实例排障图中的实例配置事件逐一进行故障排查。
- [0050] 再一方面,一种服务器,包括:
- [0051] 至少一个处理器;以及,
- [0052] 与所述至少一个处理器通信连接的存储器;其中,
- [0053] 所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行上述的运维系统排障方法。
- [0054] 又一方面,一种计算机可读存储介质,存储有计算机程序,所述计算机程序被处理器执行上述的运维系统排障方法。
- [0055] 本发明实施例提供的运维系统排障方法、装置、服务器和存储介质,提出了一个基于排障图和专家领域知识的自动化排障系统,将整个专家人工排障的流程自动化。传统的自动化排障流程需要对每一个运维实体对象进行单独的配置,这样的流程费时费力,且随着系统的升级、变更,难以有效地进行维护。因此,本方法中提出的排障引擎,将对不同的运维实体对象进行抽象,对运维实体、故障类型进行分类,通过学习专家的运维经验,将运维经验抽象成排障图,将历史的告警、故障抽象为特定的排障事件和规则。通过高度抽象的配置,结合CMDB等信息,对抽象化的排障流程进行实例化,以减少人工配置的复杂度。
- [0056] 具体的,首先,提出了一种通用的排障引擎架构,能够适用于应用、存储、网络、硬件等各个领域的运维排障问题。其次,必示排障引擎能够集中收集并展示运维需要用到的各种数据,方便运维人员查看。在此基础上,通过排障引擎中的智能异常检测方法、根因定

位、根因止损、影响力分析的算法得到具体的排障结果数据,辅助运维人员的排障工作。

[0057] 上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂,以下特举本发明的具体实施方式。

附图说明

[0058] 一个或多个实施例通过与之对应的附图中的图片进行示例性说明,这些示例性说明并不构成对实施例的限定,附图中具有相同参考数字标号的元件表示为类似的元件,除非有特别申明,附图中的图不构成比例限制。

[0059] 图1是本发明实施例提供的一种运维系统排障方法流程;

[0060] 图2是本发明实施例中运维排障系统功能结构框图;

[0061] 图3是本发明实施例提供的另一种运维系统排障方法流程;

[0062] 图4是本发明实施例抽象排障图结构示意图;

[0063] 图5是本发明实施例中基本事件和虚拟事件结构示意图;

[0064] 图6是本发明实施例中数据库异常虚拟结点结构示意图;

[0065] 图7是本发明实施例中事件配置规则结构示意图;

[0066] 图8是本发明实施例中运维系统排障装置功能结构示意图;

[0067] 图9、图10是本发明实施例中 TOP3等待事件虚拟排障图及相应实例化实例排障图;

[0068] 图11、图12是本发明实施例中TOP5等待事件虚拟排障图及相应实例化实例排障图;

[0069] 图13、图14是本发明实施例中CMDB中物理拓扑信息虚拟排障图及相应实例化实例排障图;

[0070] 图15是本发明实施例中某应用场景中虚拟排障图结构示意图;

[0071] 图16是本发明实施例中响应时间异常实例排障图结构示意图;

[0072] 图17是本发明实施例中存储排障场景实例排障图结构示意图。

具体实施方式

[0073] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合附图对本发明的各实施方式进行详细的阐述。然而,本领域的普通技术人员可以理解,在本发明各实施方式中,为了使读者更好地理解本申请而提出了许多技术细节。但是,即使没有这些技术细节和基于以下各实施方式的种种变化和修改,也可以实现本申请所要求保护的技术方案。以下各个实施例的划分是为了描述方便,不应对本发明的具体实现方式构成任何限定,各个实施例在不矛盾的前提下可以相互结合相互引用。

[0074] 本发明的第一实施方式涉及一种运维系统排障方法。其流程如图1所示,具体如下:

[0075] 101、获取排障规则数据;

[0076] 102、获取故障因果关系数据;

[0077] 103、根据排障规则数据、故障因果关系数据创建抽象排障规则,抽象排障规则包

括抽象配置事件和抽象配置规则,抽象配置事件表示虚拟排障对象,抽象配置规则表示虚拟配置事件之间的关系;

[0078] 104、获取排障知识图谱,排障知识图谱包括故障特征及相应故障原因;

[0079] 105、当排障启动条件被触发后,根据抽象排障规则、排障知识图谱生成实例排障图,实例排障图包括实例配置事件和实例配置规则,实例配置事件是实例化的虚拟事件,实例配置规则是实例化的抽象配置规则;

[0080] 106、对实例排障图中的实例配置事件逐一进行故障排查。

[0081] 本实施提供的一种运维系统排障方法,将整个专家人工排障的流程自动化。传统的自动化排障流程需要对每一个运维实体对象进行单独的配置,这样的流程费时费力,且随着系统的升级、变更,难以有效地进行维护。因此,本方法中提出的运维系统排障,首先建立通用排障规则,在具体业务场景,将对不同的运维实体对象进行抽象,对运维实体、故障类型进行分类,通过学习专家的运维经验,将运维经验抽象成排障图,由排障引擎自动执行,完成运维系统排障工作,具体的,可以将历史的告警、故障抽象为特定的排障事件和规则。通过高度抽象的配置,结合CMDB等信息,对抽象化的排障流程进行实例化,以减少人工配置的复杂度。

[0082] 作为上述实施例的一种改进,本发明实施例提供另一种运维系统排障方法。该方法由运维系统排障引擎实现,运维系统排障引擎是一种利用类树状结构将人工排障知识进行抽象、编排并自动化执行的故障分析方法,主要用于IT技术架构的系统排障,定位系统故障的原因,并推荐最好的故障止损和解决办法。参见图2,排障引擎可以按照应用、中间件、基础组件等不同领域进行组织、连接,不同的领域专家可以维护自己负责领域的排障引擎,按照实际故障场景可以将不同的领域知识编排在一起,实现快速的运维系统排障工作,主要用途为:实现IT系统的自动化排障、根因分析、修复方案推荐;对于问题事件提供影响力分析功能;将不同领域的排障知识按照统一规范进行整理和保存;综合组织多种类型的数据并集中显示,方便运维人员了解系统的健康状况。其流程如图3所示,具体如下:

[0083] 301、获取排障规则数据;

[0084] 其中,排障规则数据可以由人工输入,如运维人员可以通过配置页面完成Oracle排障规则数据的配置,并通过图形化界面进行显示。

[0085] 302、获取故障因果关系数据;

[0086] 基于历史数据,排障引擎将通过机器学习算法(FP-Growth、Pearson Correlation等)自动化挖掘各个事件之间的关联关系,对排障规则进行补充、优化。在排障规则图中,一个特定的排障事件对应图中的一个结点,两个相关联事件之间的关系则对应图中相应结点之间的一条边。由于关联事件之间存在因果关系,因此排障规则图中的边为有向边。边的方向为从原因事件指向结果事件。本发明实施例对于因果关系挖掘的算法不做限定,也非本发明所关注的创新部分,此处不再赘述。

[0087] 303、根据排障规则数据、故障因果关系数据创建抽象排障规则,抽象排障规则包括抽象配置事件和抽象配置规则,抽象配置事件表示虚拟排障对象,抽象配置规则表示虚拟配置事件之间的关系;

[0088] 抽象排障规则可以命名为抽象排障图,是排障引擎工作的基础,抽象排障图基于专家领域知识和以往的排障经验,运维人员将对不同的运维实体对象类型进行抽象,对各

运维实体上可能发生的故障类型进行分类,并建立排障的大致流程,将基本的运维经验由运维系统完成,抽象排障图是一种将专家经验抽象定义的数据结构,参见图4,综合串联了运维数据(如指标、日志等)、配置数据(CMDB知识图谱,即排障知识图谱)、检测方法(异常检测、脚本查询)等运维信息。图上的结点称为事件、边称为规则。图4表示应用成功率或者响应时间出问题,可能原因是数据库,数据库下又细分了AAS -Total、CPU利用率、内存利用率、表空间使用率。

[0089] 其中,配置数据可以包括相应抽象配置事件的原因事件、结果事件、空间关系、时间关系和权重五部分。

[0090] 304、获取排障知识图谱,排障知识图谱包括故障特征及相应故障原因;

[0091] 305、获取异常检测数据;

[0092] 306、当排障启动条件被触发后,根据抽象排障规则、排障知识图谱和异常检测数据生成实例排障图,实例排障图包括实例配置事件和实例配置规则,实例配置事件是实例化的虚拟事件,实例配置规则是实例化的抽象配置规则;

[0093] 一些可选实施例中,排障启动条件包括以下方式中的一种或多种:

[0094] 方式一、其他监控和/或告警平台的API触发;

[0095] 方式二、流式数据阈值触发;

[0096] 方式三、流式数据异常检测触发;

[0097] 方式四、其他脚本命令触发。

[0098] 抽象排障规则和实例排障图是包括节点和边的树状图,抽象配置事件和实例配置事件与节点对应,抽象配置规则和实例配置规则与边对应。

[0099] 一些可选实施例中,根据抽象排障规则、排障知识图谱生成实例排障图可以包括但不限于通过以下过程实现:

[0100] 对于每个包含子结点的节点,给每个子节点赋值一个实体对象,实体对象由相应的根结点或父结点确定。

[0101] 根据抽象排障规则图中边的类型确定子结点的实体对象。

[0102] 具体的,若边的类型为“同对象”,则子结点直接继承父结点的实体对象;若边的类型不是“同对象”,则调用相应的空间关系数据,根据父结点、子结点各自的空间类型,查找对应的实体对象。

[0103] 一些可选实施例中,如图5所示,抽象配置事件和实例配置事件包括基本事件和虚拟事件,基本事件为真实事件,虚拟事件为概念事件,每个虚拟事件链接至少一个基本事件,虚拟事件链接的任一个基本事件,只要有一个基本事件结点异常则相应虚拟事件结点异常。

[0104] 基本事件:包含检测实体、检测数据、检测方法、可视化面板四部分。

[0105] 检测实体:代表具体的机器、IP、设备等信息。

[0106] 基本用法:指定特定类型机器的具体某台主机,只针对特定的主机生效。

[0107] 高级用法:只指定实体的类型,比如实体设置为DB标签,表示所有的数据库机器,相当于通过标签方式做了实体的筛选。

[0108] 检测数据:代表指标、日志、告警、接口等数据;

[0109] 基本用法:指定特定的指标名称,比如AAS-Total,表示数据库平均会话数,可以

填写大于等于1个指标,如果是单个指标则一般使用单指标异常检测方法,多指标则使用多指标异常检测方法。

[0110] 高级用法:指定获取指标的接口或者指标的类型,在事件实例化时动态的获取对应的检测指标,生成多个事件实例,跟检测实体的高级用法类似。可以填写正则表达式,Restful接口等。

[0111] 检测方法:具体判断结点是否异常检测逻辑,常见的有单指标异常检测、多指标异常检测、日志关键字检测、匹配告警等,支持定义扩展更多的方法。

[0112] 检测方法的分析结果为正常、异常两种状态,同时包含检测报告

[0113] 可视化面板:给出结点详细的可视化风格,一般是折线图、柱状图、柄状图、日志等。不同的事件可以选择不同的可视化风格。

[0114] 需要说明的是,检测实体可以抽象成类型,可以灵活定义生效范围,可以跟CMDB管理解耦;检测数据可以抽象成类型或者接口,可以灵活定位生效范围,跟指标对象管理解耦;检测方法按灵活可扩展,可以是规则、算法、查询脚本等,跟检测逻辑解耦;支持丰富的可视化面板,灵活可扩展,可视化是事件管理解耦;结合实际CMDB信息、指标管理接口等信息,在故障时刻可以按照当前CMDB等信息自动的实例化事件,实现全方位的监控和排查。

[0115] 举例:

[0116] 基本用法:

[0117] 1. 数据库平均会话数:检测数据库实例的AAS-TOTAL是否异常,检测方法为单指标异常检测,结果为AAS-TOTAL是否为异常,同时给出详细的异常信息。

[0118] 表1 AAS-TOTAL (DB)

事件配置。	内容。
检测实体。	DB: 数据库所有实例。
检测数据。	AAS-TOTAL: 平均活动会话数指标。
检测方法。	<u>单指标异常检测</u> 。
可视化面板。	折线图。

[0119] 2. CPU利用率:检测数据库实例DB1001的CPU使用异常,检测方法为恒定阈值,这种事件只在DB1001机器生效,其他数据库机器不生效

[0120] 表2 CPU利用率 (DB1001)

事件配置。	内容。
检测实体。	数据库实例 DB1001。
检测数据。	CPU 利用率。
检测方法。	恒定阈值，大于 85%异常。
可视化面板。	折线图 + 恒定阈值基线。

[0121] 3. 数据库错误日志: 检测数据库实例的日志是否包含错误关键字, 如果包含则异常

[0122] 表3数据库错误日志 (DB)

事件配置。	内容。
检测实体。	DB: 数据库所有实例。
检测数据。	Oracle Alert 日志。
检测方法。	错误关键字检测, 比如 Ora-, Eroror, 关键字列表可配置。
可视化面板。	折线图 + 恒定阈值基线。

[0123] - 高级用法:

[0124] 1 . TOP-K等待事件分析: 数据库AAS-Total告警时, 接下来需要分析当前发生哪些等待事件, 一般只需要分析Top-K的等待事件, 实际等待事件可能无法提前配置在事件中, 需要在触发排障时动态生成, 所以检测数据需要配置成接口。事件实例化时会动态生成不同检测数据的事件实例。主要用法定位发现新的数据库等待事件。

[0125] 表4 TOP-K等待事件 (DB)

事件配置。	内容。
检测实体。	DB: 数据库所有实例。
检测数据。	等待事件类型: log file sync, buffer busy wait 等都属于等待事件。
检测方法。	<u>单指标异常检测</u> 。
可视化面板。	折线图。

[0126] 2. 新模式日志发现:实际有些新的故障无法通过之前配置模式(关键字、日志模板)的日志监控告警发现问题,需要通过一些新模式的日志定位原因。

[0127] 表5新模式日志(DB)

事件配置。	内容。
检测实体。	DB: 数据库所有实例。
检测数据。	新模式日志。
检测方法。	新模式日志发现。
可视化面板。	折线图。

[0128] 虚拟事件结点:是一种逻辑概念的事件,它链接到多个基本事件结点,只要有一个基本事件结点异常则虚拟事件结点异常。如图6所示数据库异常虚拟结点。需要说明的是,虚拟事件没有明确的检测数据,结点的状态取决于子结点;方便配置不同领域的事件的因果关系,触发领域的全流程的自动化排障;方便总结归纳问题,比如CPU异常可能是CPU USAGE、CPU IDL等多个基本事件的组合关系。

[0129] 本发明实施例中,虚拟事件为基本事件或的关系,对于多个事件的与、异或、与或组合等复杂的关系本发明实施不做过多描述,目前我们只需要或的关系,其他的关系做成单个基本结点,在检测方法中实现复杂的关系,方便维护理解。

[0130] 排障图中,关于事件配置规则对应的边,用于表达事件之间的因果关系。图7是一个事件配置规则的例子,数据库的核心指标AAS-TOTAL可能会导致相关业务的响应时间异常。

[0131] 配置事件规则:由原因事件、结果事件、空间关系、时间关系、权重五部分组成,其中,原因事件:会带来影响的事件,比如上面例子中的AAS-TOTAL事件;结果事件:为被影响的事件,比如上面例子中的响应时间事件;空间关系:表示两个事件在空间存在一定的关系;

[0132] 基本用法:通过查询物理拓扑、应用拓扑得到的关系;

[0133] 关联:查询CMDB,判断从物理拓扑上是否关联;

[0134] 同对象:两个事件属于同一个实体;

[0135] 上游业务:在业务场景中关联关系的细分,表示寻找上游业务;

[0136] 下游业务:在业务场景中关联关系的细分,表示寻找下游业务;

[0137] 高级用法:通过算法计算得到的关系;

[0138] TOP-K实体:通过脚本或者接口查询指标最大的TOP-K实体;

[0139] 多维算法:通过多维定位算法定位到具体哪些维度属性的事件有问题,输出具体的维度的虚拟事件,比如AP异常、交易码异常等;

[0140] 调用链算法:通过调用链算法,输出TOP-3的异常业;

[0141] 链路包含:属于同一个网络路径;

[0142] 时间关系:表示两个事件因果关系成立的最大时间间隔;

[0143] 权重:表示因果关系成立置信度,用于根因排序。可以人工设置或者算法学习更新。

[0144] 307、对实例排障图中的实例配置事件逐一进行故障排查。

[0145] 308、对排查出的故障信息进行根因定位,以确定故障产生的原因。

[0146] 309、图形化显示抽象排障规则,和/或,图形化显示实例排障图。

[0147] 实例化排障则是排障引擎实际的工作流程,在接收到具体的排障需求时(例如告警、异常检测结果、特定脚本等),排障引擎会根据触发条件(例如告警的具体时间、设备位置、现象),基于已配置的排障规则,自动化生成排障结果:

[0148] 1)生成排障图:在故障发生时,必示排障引擎根据已配置的抽象排障图、CMDB空间关系、实际发生故障的时间和实例等信息生成具体的实例化排障图,图中的结点为待排障的事件,边为事件之间的关系;

[0149] 2)执行排障流程:结合平时运维用到的告警、日志、指标等数据,对每一项待排障的事件,调用对应的智能检测算法排查各个事件是否异常;

[0150] 再得到每个待排障事件的异常检测结果后,排障引擎会汇总所有数据,展示排障结果。上述排障结果可以进一步被其他的上层应用使用,以展示更全面的排障结果。

[0151] 本实施提供的一种运维系统排障方法,将整个专家人工排障的流程自动化。传统的自动化排障流程需要对每一个运维实体对象进行单独的配置,这样的流程费时费力,且随着系统的升级、变更,难以有效地进行维护。因此,本方法中提出的运维系统排障,首先建立通用排障规则,在具体业务场景,将对不同的运维实体对象进行抽象,对运维实体、故障类型进行分类,通过学习专家的运维经验,将运维经验抽象成排障图,由排障引擎自动执行,完成运维系统排障工作,具体的,可以将历史的告警、故障抽象为特定的排障事件和规则。通过高度抽象的配置,结合CMDB等信息,对抽象化的排障流程进行实例化,以减少人工配置的复杂度。

[0152] 上面各种方法的步骤划分,只是为了描述清楚,实现时可以合并为一个步骤或者对某些步骤进行拆分,分解为多个步骤,只要包括相同的逻辑关系,都在本专利的保护范围内;对算法中或者流程中添加无关紧要的修改或者引入无关紧要的设计,但不改变其算法和流程的核心设计都在该专利的保护范围内。

[0153] 本发明第三实施方式涉及一种运维系统排障装置,如图8所示,包括:

[0154] 规则数据获取模块81,用于获取排障规则数据;

[0155] 因果关系获取模块82,用于获取故障因果关系数据;

[0156] 抽象规则创建模块83,用于根据所述排障规则数据、所述故障因果关系数据创建抽象排障规则,所述抽象排障规则包括抽象配置事件和抽象配置规则,所述抽象配置事件表示虚拟排障对象,所述抽象配置规则表示所述虚拟配置事件之间的关系;

[0157] 图谱获取模块84,用于获取排障知识图谱,所述排障知识图谱包括故障特征及相应故障原因;

[0158] 实例排障图创建模块85,用于当排障启动条件被触发后,根据所述抽象排障规则、所述排障知识图谱生成实例排障图,所述实例排障图包括实例配置事件和实例配置规则,所述实例配置事件是实例化的所述虚拟事件,所述实例配置规则是实例化的所述抽象配置规则;

[0159] 故障排查模块86,用于对所述实例排障图中的实例配置事件逐一进行故障排查。

[0160] 本实施提供的一种运维系统排障装置,将整个专家人工排障的流程自动化。传统的自动化排障流程需要对每一个运维实体对象进行单独的配置,这样的流程费时费力,且随着系统的升级、变更,难以有效地进行维护。因此,本方法中提出的运维系统排障,首先建立通用排障规则,在具体业务场景,将对不同的运维实体对象进行抽象,对运维实体、故障类型进行分类,通过学习专家的运维经验,将运维经验抽象成排障图,由排障引擎自动执行,完成运维系统排障工作。

[0161] 不难发现,本实施方式为与第一实施方式相对应的装置实施例,本实施方式可与第一实施方式互相配合实施。第一实施方式中提到的相关技术细节在本实施方式中依然有效,为了减少重复,这里不再赘述。相应地,本实施方式中提到的相关技术细节也可应用在第一实施方式中。

[0162] 值得一提的是,本实施方式中所涉及到的各模块均为逻辑模块,在实际应用中,一个逻辑单元可以是一个物理单元,也可以是一个物理单元的一部分,还可以以多个物理单元的组合实现。此外,为了突出本发明的创新部分,本实施方式中并没有将与解决本发明所提出的技术问题关系不太密切的单元引入,但这并不表明本实施方式中不存在其它的单元。

[0163] 由于第二实施方式与本实施方式相互对应,因此本实施方式可与第二实施方式互相配合实施。第二实施方式中提到的相关技术细节在本实施方式中依然有效,在第二实施方式中所能达到的技术效果在本实施方式中也同样可以实现,为了减少重复,这里不再赘述。相应地,本实施方式中提到的相关技术细节也可应用在第二实施方式中。

[0164] 本发明第四实施方式涉及一种服务器,包括

[0165] 至少一个处理器;以及,

[0166] 与所述至少一个处理器通信连接的存储器;其中,

[0167] 所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行上述的运维系统排障方法。

[0168] 其中,存储器和处理器采用总线方式连接,总线可以包括任意数量的互联的总线和桥,总线将一个或多个处理器和存储器的各种电路连接在一起。总线还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路连接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口在总线和收发机之间提供接口。收发机可以是一个元件,也可以是多个元件,比如多个接收器和发送器,提供用于在传输介质上与各种其他装置通信的单元。经处理器处理的数据通过天线在无线介质上进行传输,进一步,天线还接收数据并将数据传送给处理器。

[0169] 处理器负责管理总线和通常的处理,还可以提供各种功能,包括定时,外围接口,电压调节、电源管理以及其他控制功能。而存储器可以被用于存储处理器在执行操作时所使用的数据。

[0170] 本发明第五实施方式涉及一种计算机可读存储介质,存储有计算机程序。计算机程序被处理器执行时实现上述方法实施例。

[0171] 本领域技术人员可以理解,实现上述实施例方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序存储在一个存储介质中,包括若干指令用以使得一个设备(可以是单片机,芯片等)或处理器(processor)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0172] 具体排障场景

[0173] 数据库CPU场景分析:数据库实例DB1001发生CPU告警,查询到TOP3的SQL ID有ID1, ID2, ID3。最终将图9所述虚拟排障图自动实例化图10所示实例排障图。

[0174] 参见图11、图12,数据库TOP5等待事件分析:数据库实例DB1001发生AAS-TOTAL告警,自动实例化排障图,生成TOP3的等待事件,并触发后续的排查。CMDDB中物理拓扑信息:DB1001机器关联的存储是SAN1001。

[0175] 网络定位场景:CMDDB中物理拓扑信息:10.0.0.1访问11.0.0.1 80端口经过了Switch1, Router1, Switch2, Router2这些设备。具体的排障图和实例化后的排障图如图13、图14所示。

[0176] 应用排障场景:

[0177] 成功率异常场景:成功率下降一般分为两种,系统成功率下降一般原因是调用超时、报错导致的;业务成功率下降一般原因是业务上的逻辑错误,比如转账金额不对等。

[0178] 人工排障的流程:

[0179] 找到故障时刻变化量最大的错误码。

[0180] 利用TOP-K的错误码过滤交易明细数据,构建子服务的调用链,找到带错误码最根源的子服务。

[0181] 做多维定位分析,判断是内部问题还是外部问题。如果是外部问题则停止定位分析,如果是内部问题需要对根源的子服务定位他们的AP、DB、网络等具体问题。

[0182] 将人工排障流程自动化,需要配置的排障图如图15所示:

[0183] 响应时间异常：一般需要通过调用链信息定位到响应时间异常且对总耗时贡献最大的子系统，或者两个子系统的边上耗时（网络、主机队列问题）。如果定位某个系统处理时间长，需要进一步排查系统各个组件。排障图配置如图16所示：

[0184] 存储排障场景：存储排障的过程由存储SG (Storage Group) 对应的DB发生读写异常触发，首先需要确定SG的黄金指标RT和其他几个重点指标是否异常，随后去按照SG到DB的拓扑链路（存储-前端口-存储交换机-核心交换机-主机交换机-HBA卡-主机）逐个排查链路中各个实体是否发生日志或者指标异常。排障图配置如图17所示：

[0185] 本领域的普通技术人员可以理解，上述各实施方式是实现本发明的具体实施例，而在实际应用中，可以在形式上和细节上对其作各种改变，而不偏离本发明的精神和范围。

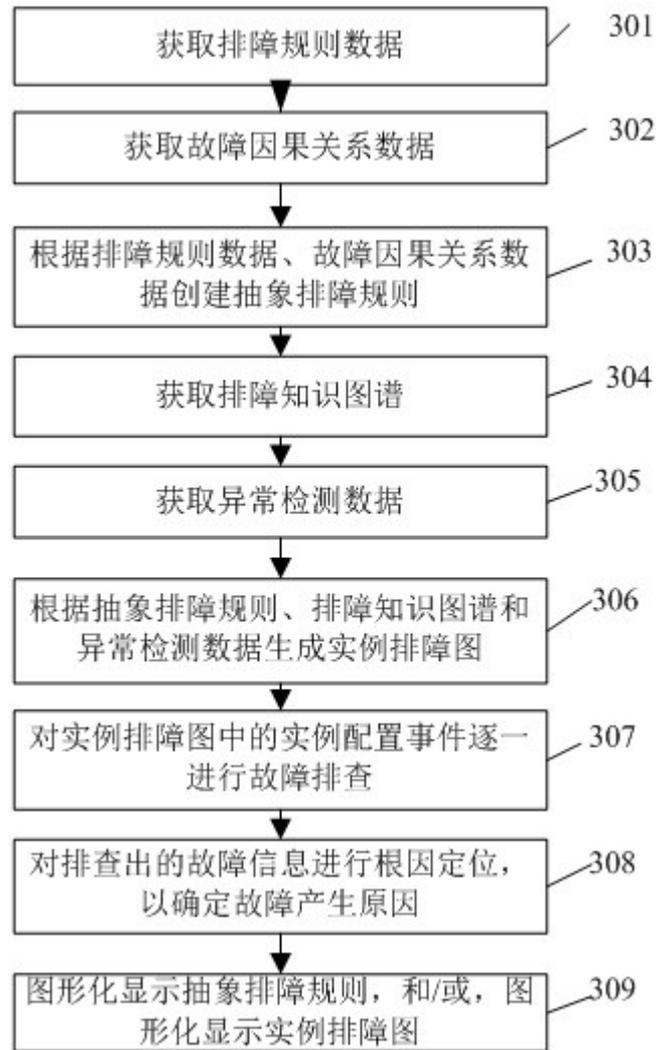


图3

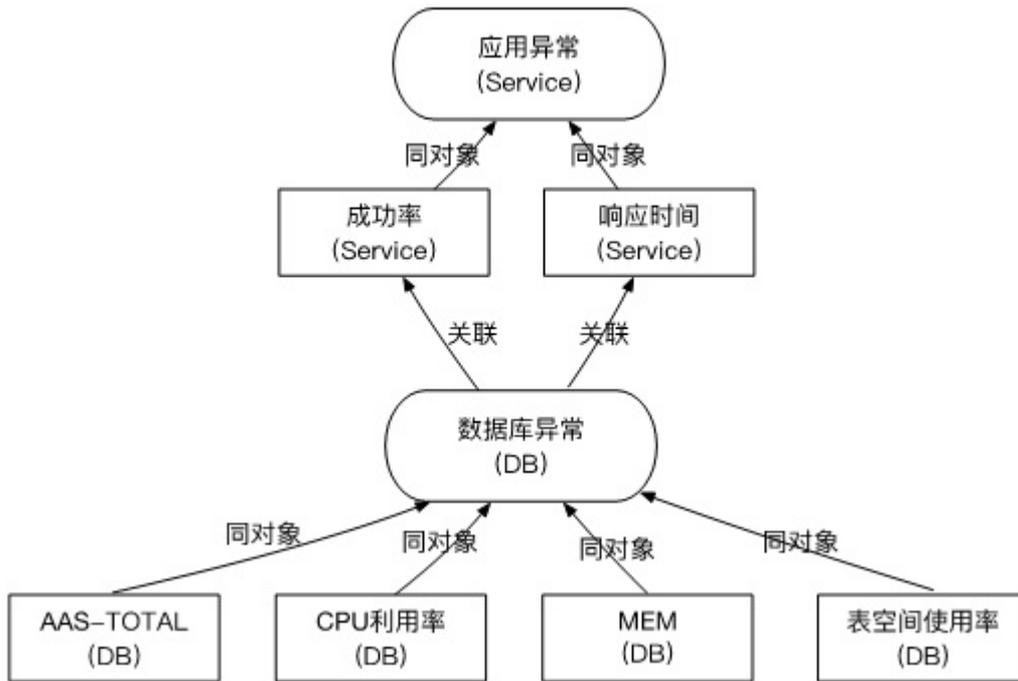


图4



图5

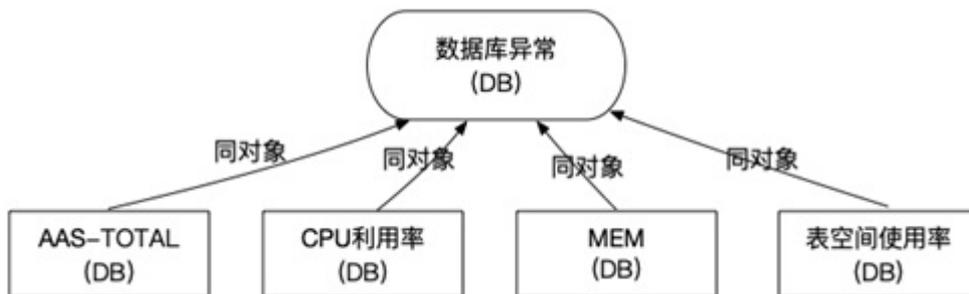


图6

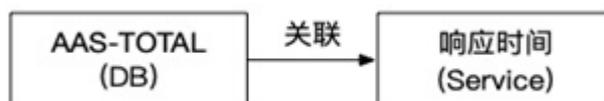


图7

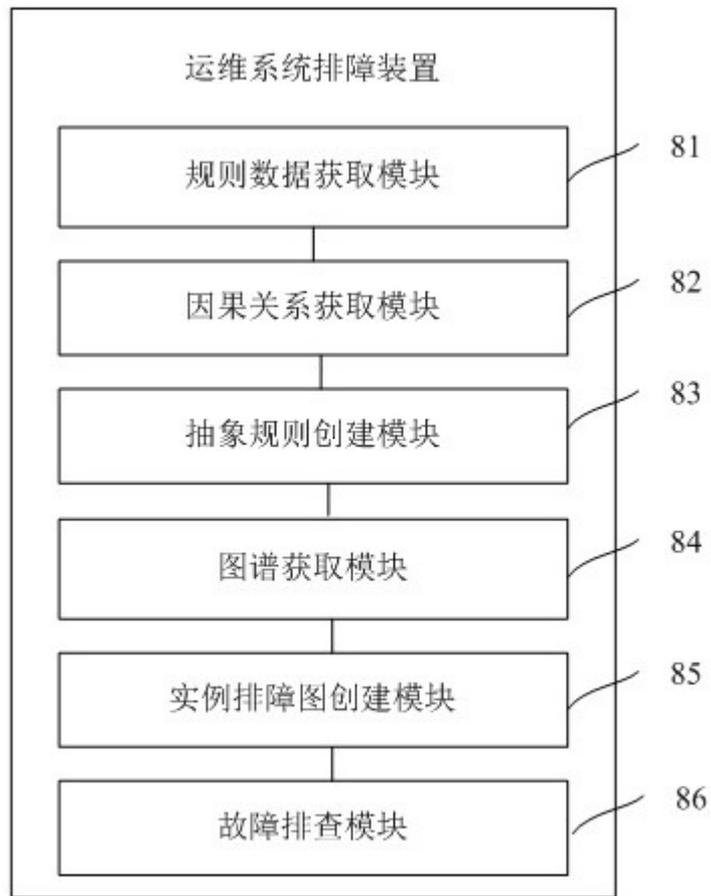


图8

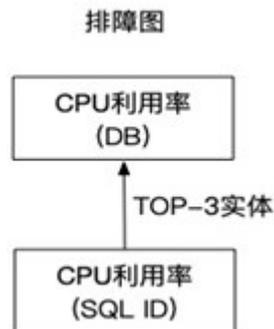


图9

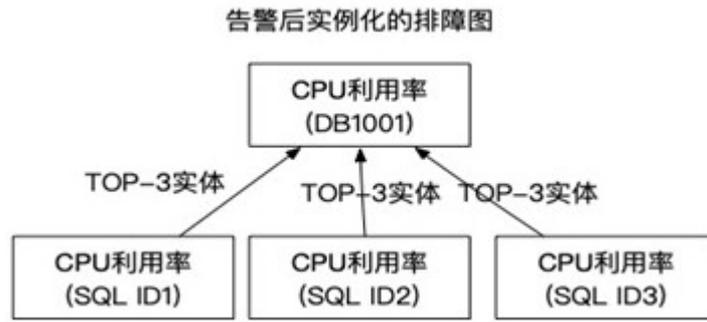


图10

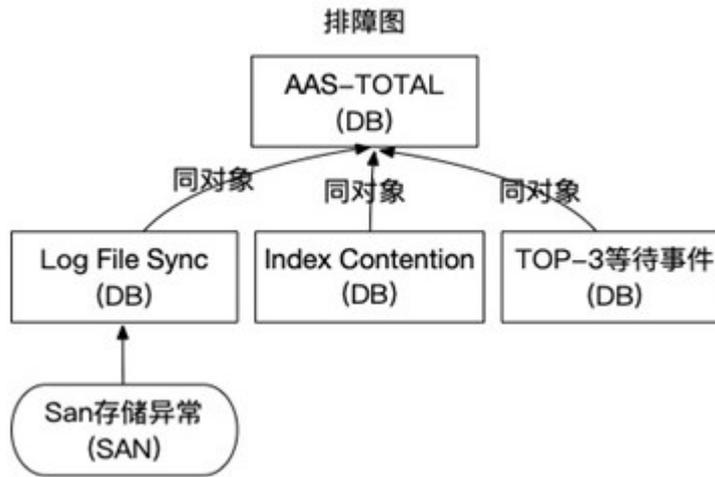


图11

告警后实例化的排障图

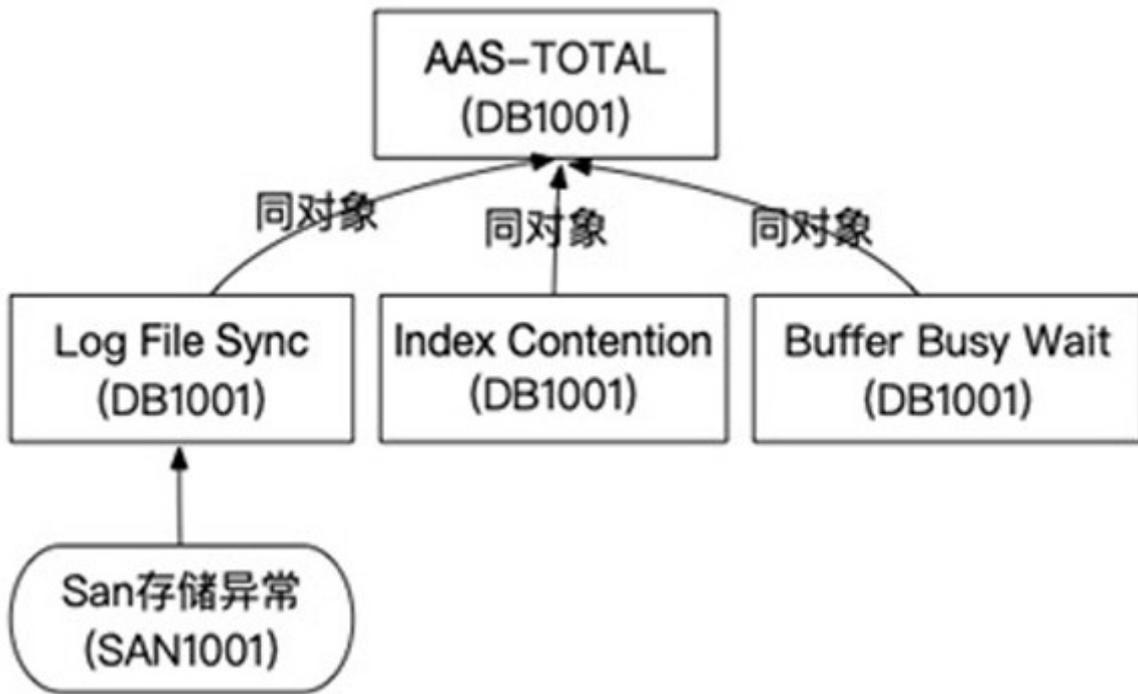


图12

排障图

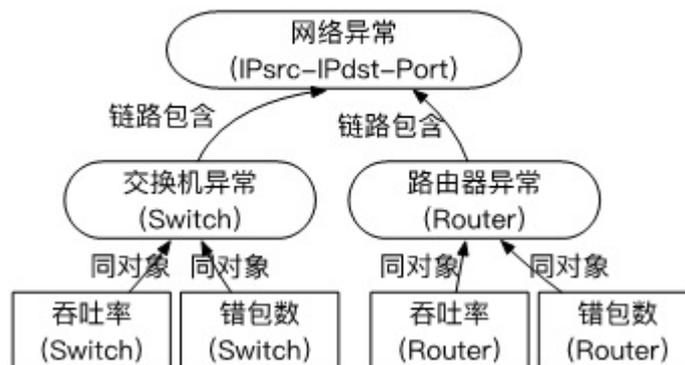


图13

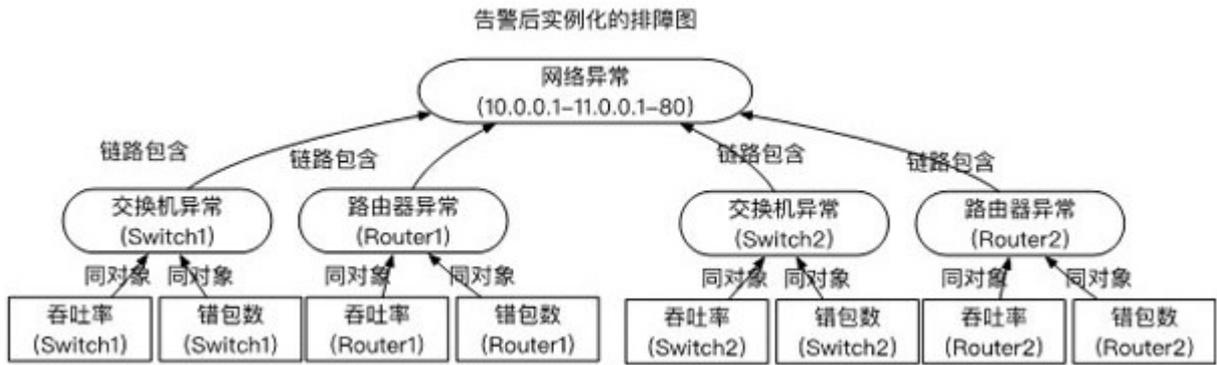


图14

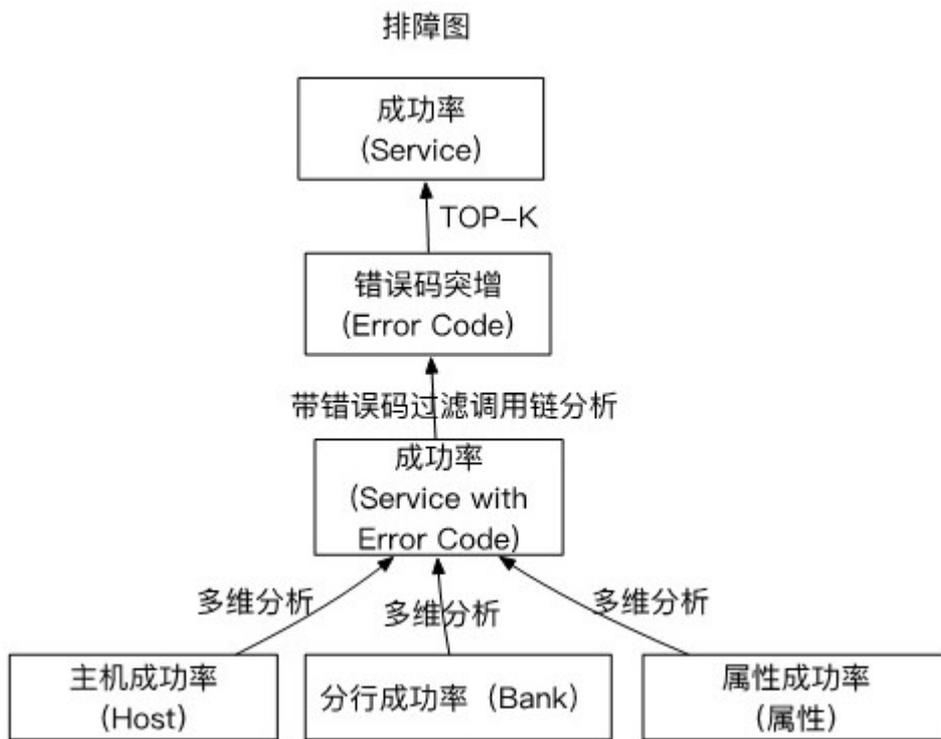


图15

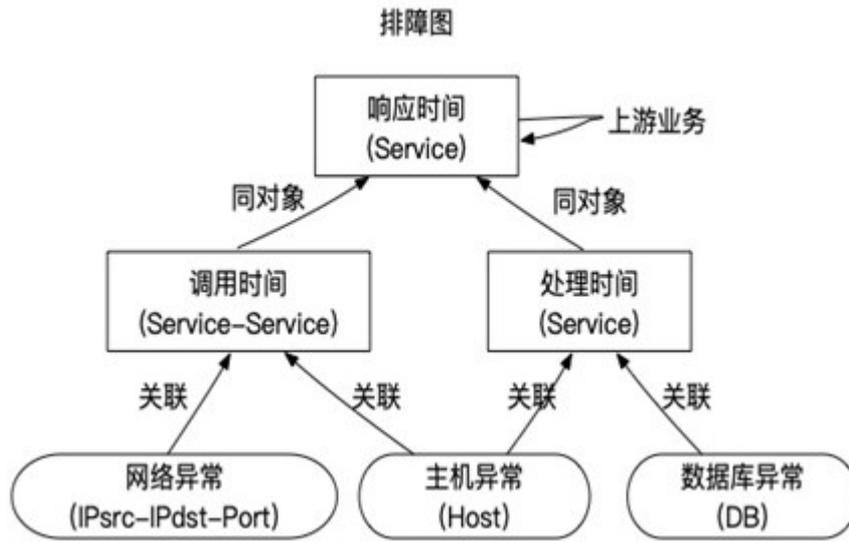


图16

