基于大数据分析的云资源池告警信息关联方案

李青
（中国电信股份有限公司研究院，上海 200135）

摘　要：研究了一种云资源池端到端智能化运维管理系统，提出一种智能判断故障模块的技术架构，分析了实现云资源池端到端告警关联的基本方法，阐述了云资源池单 KPI 异常检测分析方法和多 KPI 故障传播链分析方法的实现原理，并重点介绍了物理主机告警与虚拟主机告警、IP SAN 存储告警与虚拟对象存储告警、主机设备告警与网络告警的关联关系，为运营商提升云资源池端到端智能化运维能力提供了借鉴和参考。

关键词：云资源池；告警关联；根因分析；智能运维
中图分类号：TP307
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020141

Alarm information association scheme of cloud resource pool based on big data analysis

LI Qing
Research Institute of China Telecom Co., Ltd., Shanghai 200135, China

Abstract: An end-to-end intelligent operation and maintenance management system of cloud resource pool was studied, and a technical framework of intelligent obstacle detection module was proposed. The basic method of realizing end-to-end alarm association of cloud resource pool was analyzed. The realization of anomaly detection analysis method of single KPI and fault propagation chain analysis method of multi-KPI in cloud resource pool were expounded. The relationship between physical host alarm and virtual host alarm, IP SAN storage alarm and virtual object storage alarm, host device alarm and network alarm were introduced emphatically, which provide a reference for improving the end-to-end intelligent operation and maintenance capability of cloud resource pool.

Key words: cloud resource pool, alert correlation, root cause analysis, intelligent operation and maintenance

1　引言

随着 SDN/NFV 技术在电信运营商中的广泛应用，vCPE、vIMS/VoLTE、5G 等网络云商用化部署进度逐渐加快，传统网络运营管理手段难以有效支撑网络上云工作的开展。目前，基于 IaaS 层的 IT 硬件基础设施、Hypervisor 虚拟化软件层以及云主机（virtual machine，VM）的运行监控指标体系尚不健全，异厂商之间的指标差异大，面向云网络、云业务运维人员的端到端云告警信息关联、智能判障辅助判障工具较少，导致云故障处理周期长、效率低，对云数据中心维护支撑

收稿日期：2019−11−12；修回日期：2020−04−25

系统的处理能力带来严峻挑战。尤其，在网络云分层解耦部署模式下，运营商对网络功能虚拟化基础设施（network functions virtualization infrastructure，NFVI）层的端到端告警关联分析及智能判障等运维手段提出更高要求。

为此，需要研究引入云基础设施端到端维护的策略管理机制，建立云资源池的硬件资源管理、虚拟化资源管理、硬件资源监控、虚拟化资源监控、硬件资源故障管理、虚拟资源故障管理手段和相关指标体系，支持端到端跨层告警信息采集与自动关联，结合大数据与人工智能深度学习方法，逐步形成基于 KPI/KQI 的云资源池健康检测、快速判障及故障自愈等相关智能化运维管理能力。

2 系统架构设计

本文设计提出了一种新型云管理平台智能运维系统，能为运维人员提供一站式立体运维平台，实时监控应用、资源的运行状态，通过数百种监控指标、告警与日志信息关联分析，快速锁定故障问题根源，辅助运维人员缩短云故障的判障周期，提高云资源池维护工作效率。

新型云管理平台智能维护系统自上而下，依次包括门户管理层、智能判障层和数据采集层 3 个功能层级，其系统功能架构如图 1 所示。

（1）门户管理

主要提供与云资源池运营管理和智能维护相关的门户服务。核心模块包括 UI 呈现、用户管理、资源管理、性能管理、告警管理、决策数据建模、统计管理、日志管理、故障管理与工单管理等。

（2）智能判障

主要依据故障诊断流程、根因分析策略库等，提供告警采集信息的过滤、压缩与关联，提供告警根因分析、系统性能与故障趋势预测分析等服务。核心模块包括诊断流程编排、告警根因分析

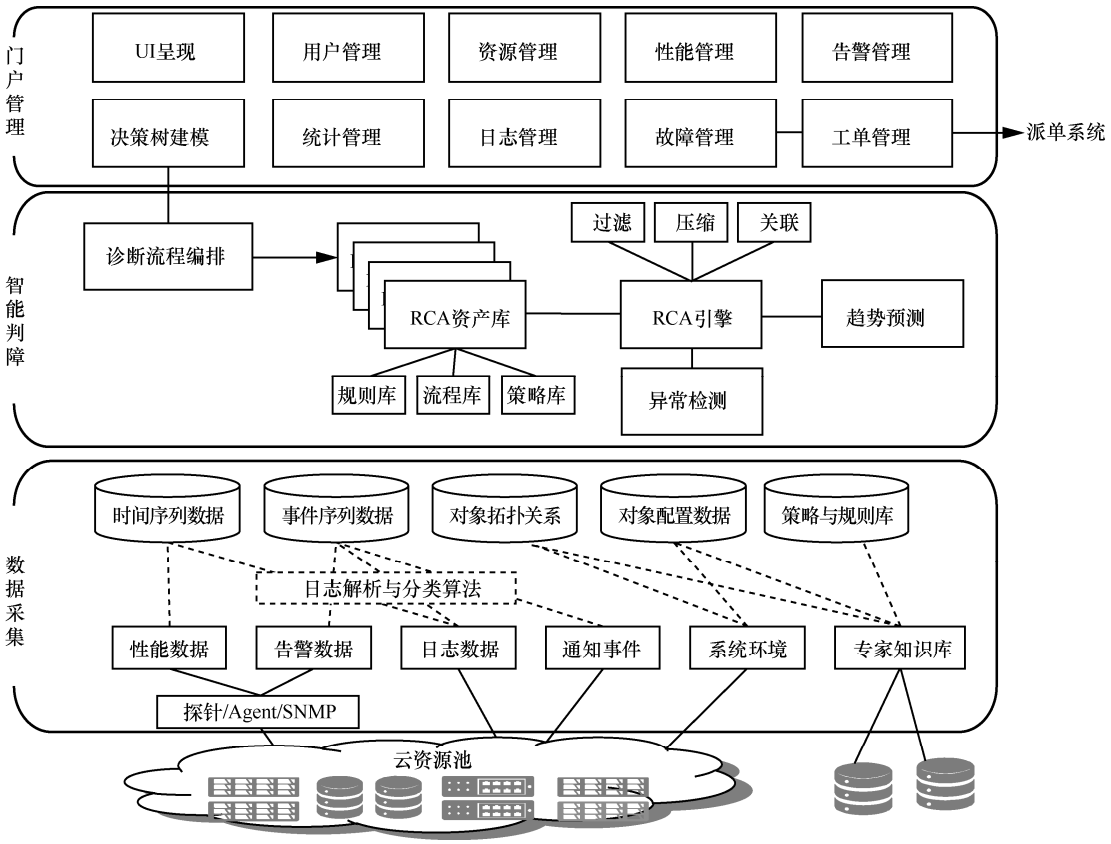

图 1 新型云管理平台智能维护系统功能架构示意图

（root cause analysis，RCA）资产库（包括规则库、流程库和策略库）、RCA 引擎（负责对采集到的告警信息进行过滤、压缩和关联处理）以及趋势预测等。

（3）数据采集

通过探针、Agent 代理（运维数据采集代理，运行在集群内各节点上，用于实时采集指标、日志等运维数据）及 SNMP（simple network management protocol，简单网络管理协议）等采集云资源池软硬件基础设施、中间件、操作系统等运行状态与告警信息，性能数据、日志数据、通知事件、环境配置数据等，并基于日志解决与分类算法，分门别类将收集到的各类数据归整为不同类型的资源池运行监控数据集群，包括时间序列数据、事件序列数据、对象拓扑关系数据、对象配置数据以及基于专家知识库的策略与规则，为智能判障提供数据与策略输入源。

3　关键技术

3.1　事件关联定义及方法分类

“事件关联”是故障智能定位的重要技术，基本思想是通过关联多个事件为某一单一概念事件过滤不必要的、不相关的事件，为云资源池管理员提供更精简的事件信息视图，以准确、快速地识别故障源。

通过分析、整理大量离散事件数据并把其关联作为一个整体进行分析，快速定位需要立即引起注意的重要告警和关键事件，从而显著简化故障检测与分析的过程。

以往事件关联重点在于减少事件数量从而简化事件管理，通常通过过滤、压缩或归纳事件。本文使用“基于状态逻辑分析”发生的事件流，同时进行模式识别以找到云资源池软硬件设施、网络设备等出现相关的问题、故障、攻击或入侵等。

实现告警“事件关联”的关键在于从各种各样的原始告警、日志、事件等海量原始数据中获取更适合人类理解的关键事件数据，自动匹配已知的故障模式或威胁模式的明确标志，找到导致故障的根本原因，从而为后继云资源池维护措施的执行、系统自愈与恢复，或云资源池网络攻击与破坏事件的检测与防护提供直接的策略指引与帮助。

（1）故障和事件的定义

事件关联的前提是对故障和事件的明确定义。本文对故障（fault）与事件（event）的定义如下。

1）故障

故障，即被云管资源池软硬件基础设施、网络设备及中间件、OS 等部件出现硬件或软件方面的问题而不能提供正常的服务。故障按其性质，可分为以下两类。

- 硬故障：芯片、主板卡、存储设备、网络卡、端口等控制器、传感器功能失效，导致系统运行异常、网络连接中断等故障，一般可通过更换硬件或调试相关软件以及重新初始化加以解决。
- 软故障：由虚拟化软件、中间件、操作系统、数据库等相关软件进程运行失常，导致死锁、挂起、资源耗尽、请求响应急速下降、访问接口或链路连接中断等问题引起的业务层应用故障。

2）事件

事件也称告警，是故障的外在表现，即被管对象出现异常后状态的改变。

事件按其性质，可分为以下两类。

- 功能性事件：被监控对象的功能失效，导致设备不再正常提供服务，无法进行通信或业务功能处理的事件。
- 性能事件：设备或进程状态虽然未挂起，但由于被管监控与故障管理相关的管理信息库（management information base，MIB）对象的值超过了预设阈值而触发的事件。例如，过高的网卡端口 IP 数据报出错率，

表明 IP 层协议实体故障。可通过设置出错率的最大阈值来触发性能事件，产生告警。

故障与事件相互联系，故障是原因，事件是结果。

告警事件易于观测和获取，但故障则通常被大量告警事件所掩盖。通过事件关联技术，可分析观测与采集到的云资源池软硬件基础设施、网络设备、中间件、数据库、操作系统等被监控对象告警信息在语义上的相关性，通过对告警、日志、事件等原始数据在时间、空间上进行相关性处理，可显著减少告警消息的数目，有助于发现引起故障的根本原因。

事件关联可分为按时间关联、按空间关联。

1）时间关联

时间关联过程，是从时间序列的角度来关联告警序列的，以便进行故障定位，形成时间序列数据库。

2）空间关联

被监控对象间的网络拓扑结构信息中显式或隐式地包含了故障告警间的关联关系。空间关联过程，是从网络拓扑结构的角度来关联告警序列的，以便进行故障定位，并形成事件序列数据、对象拓扑关系、对象配置数据等。

（2）告警逻辑相关性分类

云资源池基础设施维护具有复杂、层次化和端到端等特点，以物理主机为例，涵盖的监控对象包括 CPU、内存卡、物理硬盘、物理网卡、电源、风扇等部件以及宿主机承载的虚拟主机、虚拟网元等虚拟化设备，这些网元告警信息的出现，在物理和逻辑上都存在一定的关联性，云资源池中的独立设备故障将导致关联网元的“一点告警、多点传播”效应，而这些告警之间存在着发生时间和名称逻辑上的关联。

在关联分析中，首先需要将干扰告警进行剔除，比如将大量性能类告警（虚拟主机端口流量劣化指示、发送端口数据流量丢失等告警）中的非相关告警（CPU 温度告警等）剔除。在此筛选过程中，要兼顾重复告警可能由不同时间段的不同故障引起，不可盲目将重复告警删除，而应该结合实际故障情况进行分析甄别。因此，将此类告警进行关联归类合并处理，将大大提高集中监控效能。

1）云资源池基础设施的告警逻辑相关性分类

- 压缩处理，将多个具有同属性（例如同数据中心、同宿主机、同虚拟机等）且同时发生的告警压缩成一条告警；
- 过滤机制，剔除不符合属性相关性条件的告警；
- 累计计算，将一定数量同时发生的告警转换为新名称的告警；
- 告警抑制屏蔽，当高优先级告警产生时，则抑制低优先级告警；
- 布尔运算，将符合一定布尔运算规则的告警合称为一个告警；
- 告警泛化，通过更笼统的告警信息替换网元生成告警信息；
- 告警特化，通过更详细的告警信息替换网元生成告警信息；
- 时序关系不同的告警，按照一定的时间顺序生成。

2）云资源池端到端故障告警关联分类方式

- 衍生关联：基于各设备告警间的依存关系进行划分，分为根告警、衍生告警；
- 拓扑关联：基于云资源池各对象间的网络拓扑连接关系，分为本端告警与对端告警；
- 时间关联：基于同一故障点产生告警，具有同时间点触发特性，形成时间序列告警；
- 因果关联：由于 A 告警发生，导致 B 告警触发。例如物理主机存储卡异常，导致其虚拟机读写缓慢，形成事件序列告警；
- 链路关联：例如当云资源池汇聚层网络设备线路出现故障，将基于对象拓扑关系，

触发云资源池整个网络拓扑路径上物理设备、虚拟网元设备告警，并形成归一化告警工单。

3.2　关联算法模型

关联规则挖掘的目标是，通过分析一次故障中会同时出现的告警事件，得出一组告警事件同时出现或顺序出现的可能性，进而找出跨层告警信息项之间的关系。具体方法是，首先计算数据集中各组合项集出现的比例。当该比例超过一定的阈值时，则认为该组合是频繁出现的，组合内的成员之间可能存在一点的关联关系。最常用的是基于 Apriori 算法的关联规则挖掘模型。

（1）基本概念和定义

对于规则：A→B

项集：项的集合。包含 k 个项的项集称为 k 项集，如集合{A，B}是一个 2 项集。

- 支持度：项集 A、B 同时发生的概率为关联规则的支持度。

  Support（A→B）=P（A∪B）
- 置信度：项集 A 发生，则项集 B 发生的概率为关联规则的置信度。

  Confidence（A→B）=P（B|A）
- 最小支持度：衡量支持度的一个最小阈值。
- 最小置信度：衡量置信度的一个最小阈值。
- 频繁项集：大于或等于最小支持度的项集。
- 强关联规则：支持度和置信度均不小于最小支持度和最小置信度的规则。

（2）关联规则挖掘的两个主要内容

1）找出数据集中所有大于或等于最小支持度的频繁项集。

2）利用频繁项集生成所需要的关联规则，根据最小置信度筛选出强关联规则。

整个告警关联规则应用过程包含数据处理、算法应用和评估结果 3 部分。

首先，需对告警数据进行处理，转换为关联规则算法的数据格式。

其次，应用关联规则方法挖掘出经常一起出现的告警组合。

最后，结合真实告警场景，对得到的告警组合进行评估确认。

本文提出半自动和人工两种方式的告警关联规则挖掘方法。其中，自动关联规则挖掘方法如下。

以新型云管理平台采集到的所管辖范围内云资源池所属物理主机设备、虚拟主机、网络设备、存储设备的端到端告警数据为基础开展智能告警信息关联分析。云资源池被监控对象输出的告警信息至少包含告警 ID、告警标题、告警级别、告警开始时间、告警结束时间、告警清除时间、告警发生对象、告警归属主机、告警事件分类和告警重复次数等字段信息。

为了便于关联规则挖掘的数据格式的自动生成，采用“告警发生对象+告警标题”的字段组合，用来唯一标识一条告警数据，采用此标识方法能够将来自不同告警对象的告警信息标注为不同的告警，有利于精简告警信息和挖掘算法的高效执行。

告警唯一标识后，根据告警时间合并告警信息，形成告警事务库。另外，为了保证告警事件的连续性，需引入时间窗口和滑动步长的概念，具体如图 2 所示。

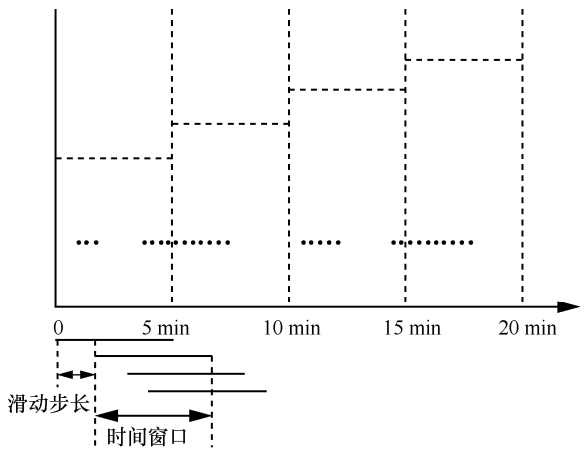

图 2　时间窗口和滑动步长示意图

图 2 中，黑色实圆点代表按时间顺序分布的离散告警事件，滑动步长可以保证一系列的告警不被截断。虽然滑动步长会导致告警重复，但这种重复在所有时间段内对于所有告警都是相同的，所以可以不予考虑。利用时间窗口和滑动步长对告警数据进行合并后，离散的告警事件则转化成某时间段内连续的告警数据库。

结合云资源池半年期 M 条历史告警数据，设置时间窗口为 T min（例如 5 min），滑动步长为 L min（例如 1 min）。根据告警清除时间与告警开始时间合并告警后，离散告警转化为 5 min 内发生的告警事务库。如果 5 min 内只有一条告警，那么则认为该时间段内，该告警的出现短时间内不会触发其他告警，予以剔除。

告警数据合并成 N 个告警事务库，这些告警事务库用于告警关联规则的挖掘。告警组合关系生成后，先使用关联规则挖掘算法得到全部的频繁项集，再利用得到的频繁项集筛选出满足最小置信度阈值的告警强关联规则。

最小支持度和最小置信度的阈值选择是关联规则中较为重要的一步，可分别尝试多种不同的最小支持度和最小置信度取值。

- 最小支持度=0.03，最小置信度=0.7，在此设定下，得到 X_1 条告警关联规则。
- 最小支持度=0.04，最小置信度=0.7，在此设定下，得到 X_2 条告警关联规则。
- 最小支持度=0.05，最小置信度=0.5，在此设定下，得到 X_3 条告警关联规则。
- 最小支持度=0.05，最小置信度=0.7，在此设定下，得到 X_4 条告警关联规则。

具体实施中，应结合实际告警场景，分别对上述告警关联规则的告警组合合理性进行人工确认。确保告警规则的完整性和合理性。

例如，根据人工确认，最终选定的最小支持度为 0.04，最小置信度为 0.7。该告警关联规则表明，对于每一条告警关联规则，在 5 min 内其中一条或多条告警的发生触发了其余告警发生的概率为 70%。

根据以上分析过程，可从云资源池维护监控平台提取的半年历史告警数据中，挖掘获得 X_2 条告警关联规则。同时，逐条确认告警关联规则合理性，剔除与实际告警场景不符合的规则。

由于历史告警信息源来自真实生产系统，与确认筛选后的每条规则中多条出现的告警均有关联。因此，基于历史告警数据分析获得的规则库，可直接应用于现网云资源池端到端智能维护，挖掘所使用的方法和结果可直接或少量修改，将挖掘得到且已被证实的告警关联规则加入到关联规则知识库，应用于实际的云资源池监控告警管理系统。

以上获得告警关联规则，一方面，可应用于告警根源定位分析。根据告警关联规则知识库，提取根源告警，快速解决告警根因问题。另一方面，也可应用于对部分告警事件的预测。根据云资源池发生的某一告警，通过匹配告警关联知识库，预测未来 5 min 内可能出现的其他告警，从而及时对告警事件做出合理处置，提高日常维护效率。

除了上述基于 Apriori 算法思路“产生－测试”的关联规则挖掘方法外，本文在部分告警信息场景下的关联规则挖掘中，还借鉴了 FP（frequent pattern，频繁模式）-Growth 算法。该算法使用一种称作 FP 树的紧凑数据结构组织数据，能直接从 FP 树结构中提取频繁项集。在整个算法执行过程中，只需遍历数据集 2 次，即可完成频繁模式发现，算法效率更高。

4 智能运维解决方案

4.1 单 KPI 异常检测分析方案

基于数理统计算法，对云资源池的物理宿主机、存储设备、网络设备以及虚拟化主机设备等相关的云数据中心软硬件基础设施任意 KPI 进行

采样，并做数据变动基线分析，对周期性变化指标可基于自学习方法展示其周期性变化的规律基线，对超过阈值基线的事件进行告警。

4.1.1　KPI 历史基线检测

单 KPI 历史基线检测方案适用于有容量限制的 KPI、随着时间单向递增或递减的 KPI、周期性变化很小的 KPI、指标波动规律与时间强相关的 KPI 以及纳入考核达标要求的 KPI 等。单 KPI 指标历史基线检测示意图如图 3 所示。

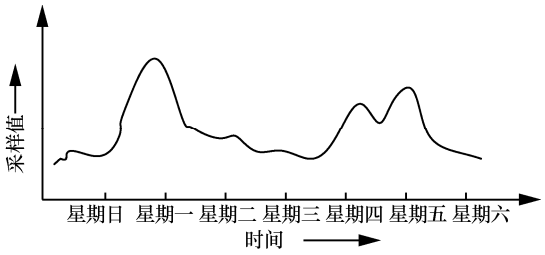

图 3　单 KPI 历史基线检测示意图

本文研究提出以下 4 个类型的单 KPI 及监控策略。

（1）有容量限制的指标（静态基线）

- 容忍线：对于容量类（例如最大并发进程数、并发用户连接数、并发 session 等）告警，可以只设定高容忍线。
- 监控策略：设置多个超出时限，逐级升级告警。

（2）随时间单向递增或递减的指标（静态基线）

- 容忍线：对于资源使用量类指标（例如磁盘利用率、磁盘空间、数据库表空间、磁盘可使用天数、文件系统空间使用率等），可以在指标变化趋势的方向上设置单侧容忍线（上容忍线或下容忍线）。
- 监控策略：设置上/下容忍线（可设置多个超出时限、逐级升级告警），或者根据历史使用数据，采用线性回归算法，计算使用速率，估算空间的剩余可使用天数。

（3）周期性变化很小的指标（动态基线）

- 容忍线：对于命中率、部分使用率（例如缓冲区命中率（%）、高速缓冲区命中率（%）、读请求磁盘命中率（%）、写请求磁盘命中率（%）等），或者响应类的通用指标（例如响应时间、线程个数等），可以只设定上容忍线或者下容忍线。
- 监控策略：根据历史数据，采用正态分布算法，设置合理的超出时限。

（4）指标波动与时间相关，随时间变化呈规律性波动（动态基线）

- 容忍线：对于大部分周期性的指标（例如 CPU 使用率、内存使用率、网卡端口接收速率、网卡端口发送速率），可同时设置上容忍线和下容忍线。
- 监控策略：根据正态分布算法，设置周期变化的阈值。

（5）纳入 KPI 考核达标要求的指标（静态基线）

- 容忍线：对于运营考核类 KPI，设置单侧达标容忍线（高容忍线或低容忍线）。
- 监控策略：可设置固定值，超出固定值产生告警。

基于时序的 KPI 建模与分析方法有两方面的使用价值。

（1）预测未来云资源池运行质量，为云资源池运行质量与客户体验优化提供依据。

（2）用于异常告警检测。当实际值与预测值相差较大时，可认为云资源池运行状态即将或已经出现异常，为故障预测告警和快速诊断提供判障依据。

具体应用如图 4 所示。单 KPI 行为历史轨迹的自学习和分析围绕其变动基线展开，阈值基于指标采样数据的波动规律自动生成，越值则自动判定并告警。

4.1.2　KPI 周期曲线分析

在现网生产环境中，虽然诸多 KPI 在时间特征序列上具有明显的周期性，但由于 KPI 数据变化趋势受用户业务行为的随机性、突发事件等影

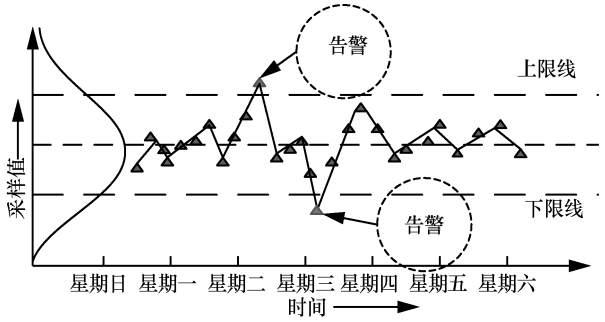

图 4　KPI 历史基线检分析与阈值测告警示意图

响，单纯依靠单一上下线 KPI 阈值的判定方法，容易形成误告警，影响告警的准确性。因此，可利用周期性季节时间序列（seasonal ARIMA，SARIMA）模型，从时间序列的随机性、平稳性和季节性 3 个方面考虑，借助自相关系数以及偏相关系数分析方法，在 KPI 历史基线分析方法基础上进行改进，形成 KPI 周期曲线模型评估模型。如图 5 所示。

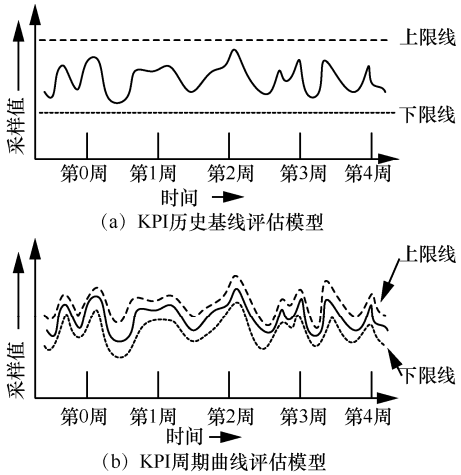

图 5　KPI 周期曲线分析方法示意图

4.1.3　KPI 异常预警处理流程

云资源池端到端智能运维解决方案中，KPI 异常预警流程分为以下 4 个步骤。

（1）KPI 历史基线自学习

针对云资源池物理宿主机、存储设备、网络设备、虚拟化主机及存储对象等的性能、告警、日志、事件通知等，采集各项 KPI 历史数据，根据时间序列形成历史基线。

（2）动态生成 KPI 周期曲线

引入自学习算法，考虑时间序列的随机性、平稳性和季节性等因素，借助自相关系数以及偏

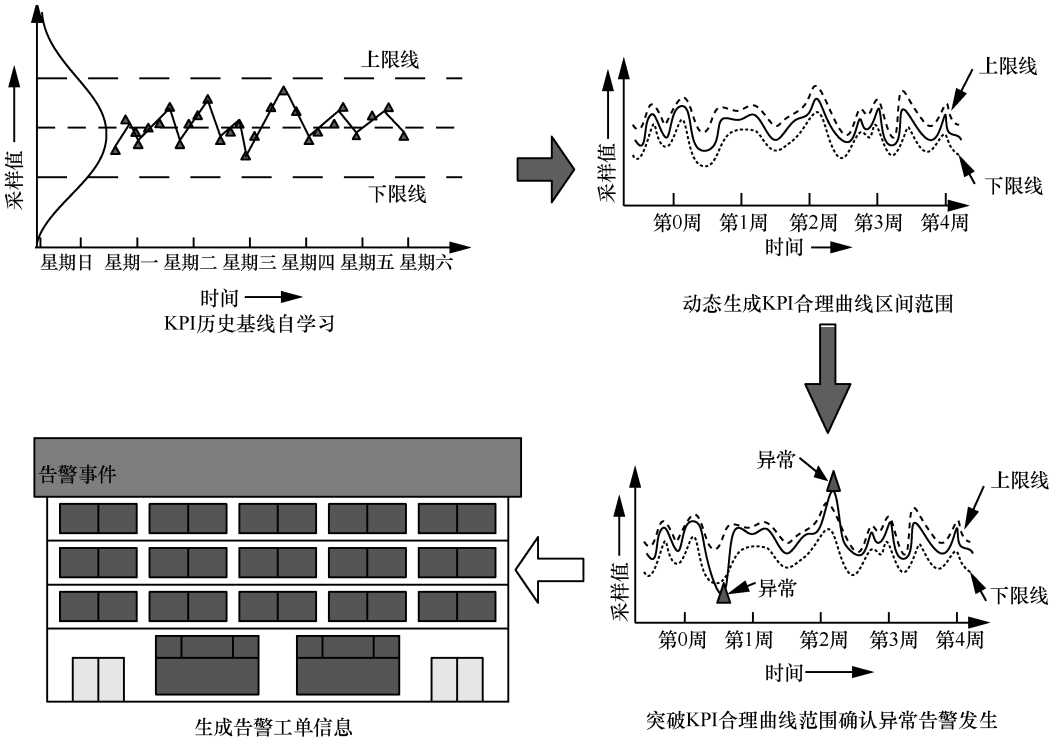

图 6　KPI 异常预警流程示意图

相关系数分析方法，基于 KPI 历史基线，动态生成 KPI 曲线运行的合理区间包线范围。

（3）KPI 异常自主判断

对于显著超过 KPI 合理曲线区间范围的指标，进行自动判断与告警。

（4）KPI 异常告警

告警事件生成后，向网管监控系统进行告警显示生成故障处理工单，通知维护人员及时处理和响应。

4.2 故障传播链分析解决方案

基于“故障传播链”的分析模型提升是智能运维手段能力的另一重要工具，该模型从“空间维度”，对多 KPI 的衍生关系、拓扑关系、因果关系、链路关系等相关性进行分析，基于大数据分析和相关算法可自学习 KPI 间（多变量）因果关系。对于被关注的 KPI 数据，系统自学习并识别各指标之间是否有相关性。若有相关性，则系统自学习其数据变化，识别出这些指标之间“正常”的相关行为模式，并持续对其行为进行跟踪并提供图形化的展现，如图 7 所示。

可直观获得云资源池软硬件基础设施、网络设备、中间件、数据库、操作系统等被监控对象告警信息在语义上的相关性，通过对告警、日志、事件等原始数据在时间、空间上进行相关性处理以及压缩、过滤、拟制等手段，显著减少云资源池告警消息的数目，快速定位引起故障的根本原因。

4.2.1 物理主机与虚拟机告警关联分析场景

基于云资源池运营管理系统的历史告警信息，本文归纳分析了物理主机与虚拟机（以 VMWare 的 vSphere 为例，华为、新华三等虚拟化软件系统的告警信息类似）告警强关联的 8 种典型场景。

（1）场景 1：物理主机内存超载预警

物理主机内存占用率超过阈值（例如≥ 90%），导致系统运行速度慢或计算节点负载过高。与其关联的虚拟主机运行状态及告警信息如下。

1）虚拟主机状态：主机内存工作负载处于严重级别；主机内存争用处于严重级别；>50%子虚拟机存在“主机内存工作负载处于严重级别”等情况。

2）典型虚拟主机告警信息：独立主机存在由多数虚拟机导致的内存争用；由于虚拟机群太多，独立主机存在内存争用等类似告警。

（2）场景 2：物理主机 CPU 超载预警

物理主机 CPU 占用率超过阈值（例如≥

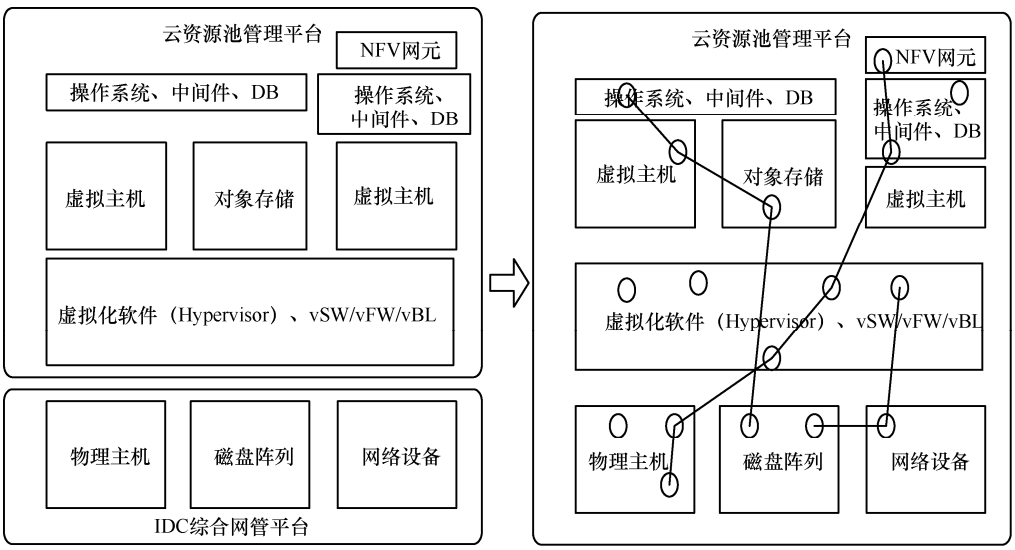

图 7　故障传播链分析方法示意图

90%），物理主机业务繁忙负载过重。与其关联的虚拟主机运行状态及告警信息如下。

- 虚拟主机状态：主机 CPU 争用处于严重警告；主机 CPU 需求处于严重级别；>50% 子虚拟机存在“主机 CPU 需求处于严重级别”等情况。
- 典型虚拟主机告警信息：独立主机存在由多数虚拟机导致的 CPU 争用；由于虚拟机群太多，独立主机存在 CPU 争用等类似告警。

（3）场景 3：物理主机磁盘可用空间预警

主机逻辑磁盘占用率超过阈值（例如≥95%），系统的性能下降，并且无法存储系统新产生的数据。与其关联的虚拟主机运行状态及告警信息如下。

- 虚拟主机状态：虚拟机磁盘 I/O 工作负荷处于严重级别；虚拟机磁盘读取滞后时间处于严重级别；虚拟机磁盘写入滞后时间处于严重级别；vSphere HA 没有足够的资源启动虚拟机的情况等。
- 典型虚拟主机告警信息：虚拟机具有意外的高磁盘 I/O 工作负载；虚拟机存在磁盘 I/O 读取滞后；虚拟机存在磁盘 I/O 写入滞后；vSphere HA 没有足够的资源启动虚拟机等类似告警。

（4）场景 4：物理主机网卡端口异常

该网口所在主机与其他相连设备通信中断，与其关联的虚拟主机运行状态及告警信息如下。

- 虚拟主机状态：主机网络数据接收工作负载处于警告级别；主机网络数据传输工作负载处警告级别；物理网卡链接状态不稳定（故障症状）；物理网卡链接状态关闭（故障症状）等情况。
- 典型虚拟主机告警信息：主机出现丢弃大量已接收的数据分组问题；主机出现丢弃大量已传输的数据分组问题；ESXi 主机检测到物理网卡上的链路状态“抖动”；ESXi 主机检测到物理网卡上的链路状态关闭等类似告警。

（5）场景 5：物理主机物理盘读写异常

物理主机的磁盘 LUN 物理故障，与其关联的虚拟主机运行状态及告警信息如下。

- 虚拟主机状态：硬盘传感器运行状态显示为红色。
- 典型虚拟主机告警信息：存储传感器正在报告问题；存储设备的路径冗余已降级等类似告警。

（6）场景 6：物理主机电池异常

物理主机的电池工作状态异常，与其关联的虚拟主机运行状态及告警信息如下。

- 虚拟主机状态：电池传感器运行状态显示为红色。
- 典型虚拟主机告警信息：电池传感器正在报告问题等类似告警。

（7）场景 7：物理主机风扇异常

物理主机的风扇工作状态异常，与其关联的虚拟主机运行状态及告警信息如下：

- 虚拟主机状态：风扇传感器运行状态显示为红色。
- 典型虚拟主机告警信息：风扇传感器正在报告问题等类似告警。

（8）场景 8：物理主机主板温度异常

物理主机的主板温度异常，与其关联的虚拟主机运行状态及告警信息如下。

- 虚拟主机状态：系统主板传感器运行状态为红色，温度传感器运行状态为红色。
- 典型虚拟主机告警信息：系统主板传感器正在报告问题，温度传感器正在报告问题等类似告警。

4.2.2 告警信息关联分析过程

以 FP-growth 算法为例，针对收集到的云资源池告警信息，进行关联规则的频繁项集挖掘，分析告警关联项，基本过程主要分为以下两个步

骤：构建 FP 树；从 FP 树中挖掘频繁项集。

4.2.2.1　构建 FP 树

先检索一遍故障告警数据库集，得到频繁项为 1 的告警项目集，定义最小支持度（告警项目出现最少次数），删除那些小于最小支持度的告警项目，然后将原始故障告警数据库集中的条目，按告警项目集中的降序进行排列。

第二次检索，创建项头表（从上往下降序）以及 FP 树。

对于每个告警项目（可按照从下往上的顺序）找到其条件模式基（conditional patten base，CPB），递归调用 FP 树结构，删除小于最小支持度的项。如果最终呈现单一路径的树结构，则直接列举所有组合；非单一路径的，则继续调用 FP 树结构，直到形成单一路径即可。

以故障告警事件清单（第一列为故障 ID，第二列为告警事件代码）为例，见表 1，说明关联告警事件的挖掘分析过程。

表 1　故障告警事件清单（样表）

故障 ID	告警事件
Fault1	A1、A2、A5
Fault2	A2、A4
Fault3	A2、A3、A6
Fault4	A1、A2、A4
Fault5	A1、A3、A7
Fault6	A2、A3、A8
Fault7	A1、A3
Fault8	A1、A2、A3、A5

（1）构建 FP 树

1）检索故障告警事件数据库/集，对每个告警事件发生的次数进行计数。

表 2　故障告警事件计数

告警事件	A1	A2	A3	A4	A5
告警次数/次	6	7	6	2	2

2）设定最小支持度（即告警最少出现的次数）为 2。

3）按降序重新排列告警事件数据集（对于计数小于 2 的告警事件删除）。

表 3　故障告警事件计数（降序）

告警事件	A2	A1	A3	A4	A5
告警次数/次	7	6	6	2	2

4）根据项目（告警）出现的次数重新调整故障告警清单。

5）构建 FP 树。

首先，加入第一条故障告警事件清单（A2, A1, A5），如图 8 所示。

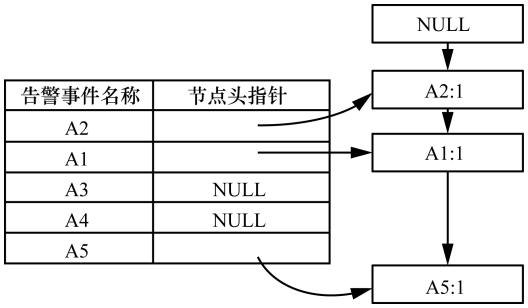

图 8　加入 Fault1 故障告警事件后构建的 FP 树

其次，加入第二条故障事件清单（A2, A4）：出现相同的节点进行累加（A2）。

再次，逐步加入第 3～9 条故障告警事件清单项目，最终得到 FP 树，如图 9 所示。

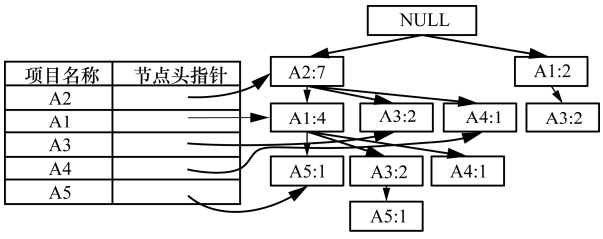

图 9　加入 Fault1~9 故障告警事件后构建的 FP 树

4.2.2.2　挖掘频繁项集

对于每一个元素项，获取其对应的条件模式基（CPB）。条件模式基是以所查找元素项为结尾的路径集合。每一条路径都是一条前缀路径。按

照从下往上的顺序排列。

例如，以告警事件 A5 为例，得到的条件模式基为{(A2 A1:1), (A2 A1 A3)}，其构造条件 FP 树如图 10 所示。

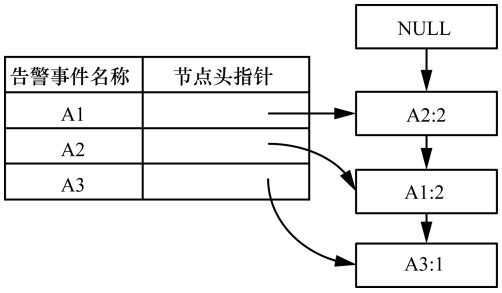

图 10　告警事件 A5 的构造条件 FP 数

然后，递归调用 FP-growth 算法，模式后缀为 A5。由于这个条件 FP 树是单路径的，因此，在 FP-growth 中直接列举{A2:2，A1:2，A3:1}的所有组合。之后，与模式后缀 A5 取并集，最终得到支持度大于 2 的所有模式：{A2 A5:2, A1 A5:2, A2 A1 A5:2}。

以此类推，可根据 FP-growth 算法，得到所有告警事件的支持度大于 2 的频繁模式，见表 4。

表 4　基于 FP-growth 算法的频繁模式

项目	条件模式基	条件 FP 树	产生的频繁模式
A5	{(A2 A1:1),(A2 A1 A3:1)}	(A2:2,A1:2)	A2 A5:2,A1 A5:2, A2 A1 A5:2
A4	{(A2 A1:1), (A2:1)}	(A2:2)	A2 A4:2
A3	{(A2 A1:2), (A2:2), (A1: 2)}	(A2:4,A1:2), (A1:2)	A2:A3:4,A1 A3:4, A2 A1 A3: 2
A1	{(A2:4)}	(A2:4)	A2 A1: 4

依据表 4，便可获得云资源池故障告警列表（样例库）中，物理宿主机、虚拟主机的各告警事件间的关联关系（例如 A5 告警出现时，会伴随发生 A1、A2 告警，或者同时发生），可依据告警信息关联关系，屏蔽干扰告警、进一步挖掘故障根因，从而简化云资源池故障告警分析过程，提高维护人员的云故障定位效率。

随着告警关联规则库的不断迭代更新和完善，为基于 AI 技术的自动故障分析、故障自愈等智能化运维手段的引入奠定基础条件。

5　结束语

近年来，国内外各大电信运营商均提出了基于 SDN/NFV 技术的网络重构战略，网络上云成为未来网络发展与演进的必然趋势。未来网络采用分层解耦部署模式后，一方面，使得网络架构更加简洁、敏捷、集约、开放，能够更加灵活地适应面向“互联网+”的业务弹性发展需求；另一方面，也使得网络运营运维工作变得更加复杂。建立物理资源、虚拟资源以及 NFV 网元的告警信息间的端到端自动关联系统，有助于快速提升网络云维护效率。

本文针对物理资源与虚拟资源间的故障告警场景进行了专题梳理，提出了基于故障传播链的告警关联分析基本方法和典型关联模型。经过现网应用验证，相关典型故障的根因定位效率提升 50%以上，从试点前的小时级提升至分钟级，显著缩短了故障定位周期。下一步，将在持续丰富告警关联案例库的同时，引入 AI 机器自学习算法，进一步提升故障根因自动定位的准确率，探索典型故障场景下的故障自愈可行性和有效性，提升基于 SDN/NFV 技术的网络云基础设施智能化运维水平。

参考文献：

[1] 张柳. 云环境下网络告警管理系统设计[D]. 南京: 南京邮电大学, 2015.
ZHANG L. Design of network alarm management system in cloud environment[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2015.

[2] 张学红, 闫五四, 李永春, 等. 基于序列模式挖掘的网管告警系统[J]. 电信科学, 2006, 32(11): 29-32.
ZHANG X H, YAN W S, LI Y C, et al. Network management alarm system based on sequential pattern mining [J]. Telecommunication Science, 2006, 32 (11): 29-32.

[3] 王新苗, 晏蒲柳, 黄天锡. 网络管理告警数据库中时序规则

挖掘的一种新方法[J]. 小型微型计算机系统, 2001, 19(11): 1311-1314.
WANG X M, YAN P L, HUANG T X. A new method of mining time series rules in network management alarm database [J]. Minicomputer System, 2001, 19(11): 1311-1314.

[4] VMware Inc. Vrealize-operations-manager-67-api-guide[S]. 2018.

[5] VMware Inc. Vrealize-operations-manager-67-reference-guide[S]. 2018.

[6] 李岩, 吴国文. SVM-SMO 算法分析及在运维中的应用[J].智能计算机与应用, 2018, 3(2): 78-80.
LI Y, WU G W. SVM-SMO algorithm analysis and application in operation and maintenance[J]. Intelligent Computer and Application, 2018, 3 (2): 78-80.

[7] CSDN. FP-growth 算法理解和实现[EB]. 2018.
CSDN. FP growth algorithm understanding and implementation[EB]. 2018.

[8] 崔力民, 何清素, 王俊生, 等. 基于二分图模型的通信信息网络故障联合定位[J]. 电信科学, 2017, 33(3): 76-82.
CUI L M, HE Q S, WANG J S. Joint fault location of communication information network based on binary graph model [J]. Telecommunication Science, 2017, 33(3): 76-82.

[9] 刘军, 楚家辉. 基于网络拓扑结构的告警事件关联分析算法研究[J]. 数字技术与应用, 2017 (4): 144.
LIU J, CHU J H. Research on alarm event correlation analysis algorithm based on network topology[J]. Digital Technology and Application, 2017(4): 144.

[10] 毛斌宏, 阳志明. NFV 故障关联及故障自愈方案研究[J]. 电信科学, 2017, 33(11): 186-194.
MAO B H, YANG Z M. Research on NFV fault correlation and fault self-healing scheme[J]. Telecommunication Science, 2017, 33(11): 186-194.

[11] 熊云艳, 毛宜军, 丁志. 安全事件关联分析引擎的研究与设计[J]. 计算机工程, 2006, 32(13): 280-282.
XIONG Y Y, MAO Y J, DING Z. Research and design of security event correlation analysis engine [J]. Computer Engineering, 2006, 32(13): 280-282.

[12] 王洋, 满毅, 陈志鹏. 基于集中监控数据资源的 4G 基站退服故障预警模型[J]. 电信科学, 2016, 32(7): 188-196.
WANG Y, MAN Y, CHEN Z P. Early warning model of 4G base station service failure based on centralized monitoring data resources[J]. Telecommunications Science, 2016, 32(7): 188-196.

[13] 孙娟, 石秋华. 对 FP-Growth 算法的一种改进算法[J]. 软件导刊, 2012, 11(1): 62-64.
SUN J, SHI Q H. An improved algorithm for FP growth algorithm [J]. Software Guide, 2012, 11(1): 62-64.

[作者简介]

李青（1973– ），男，中国电信股份有限公司研究院高级工程师，核心网与平台领域高级专家，中国电信集团 B 级人才，主要从事电信增值业务平台及产品开发、网络演进、云计算/大数据等运营技术研究工作。