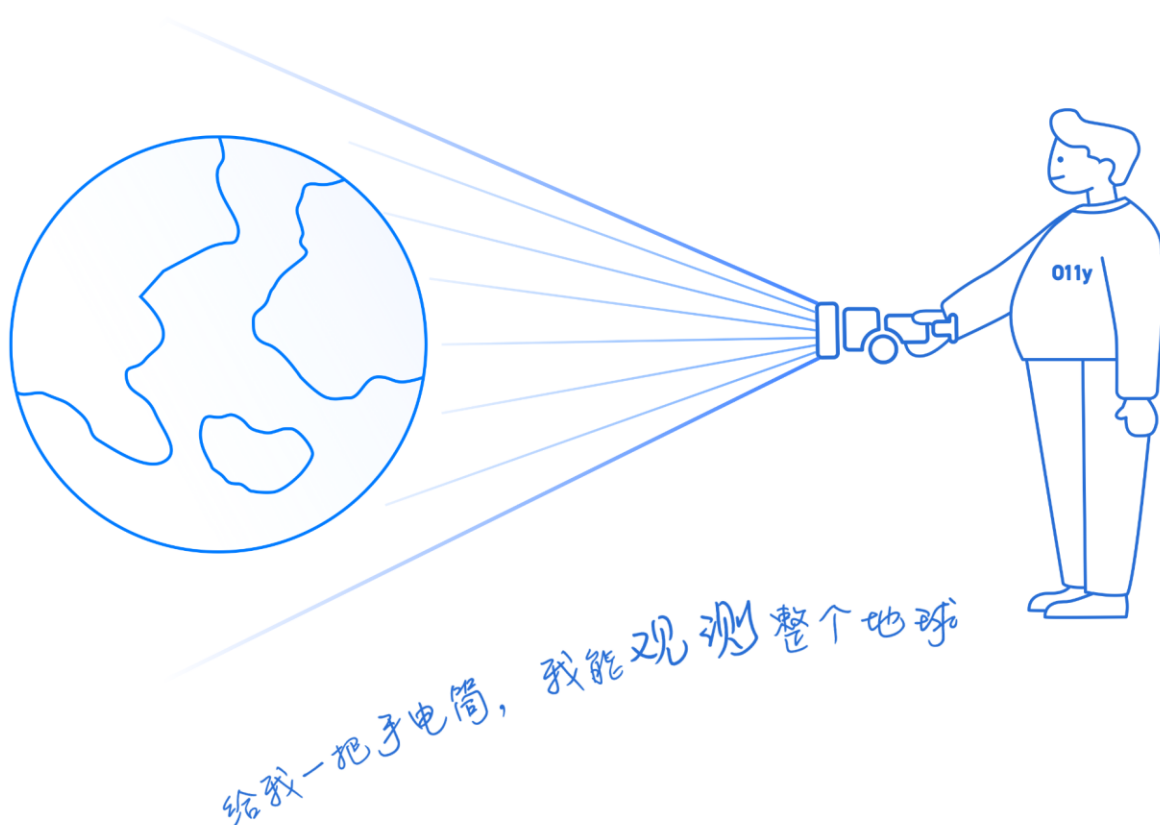


(2023年)

可观测性成熟度模型

白皮书



版权声明

本白皮书版权属于稳定性保障实验室、北京爱分析科技有限公司、龙蜥社区、国网上海电力信通公司、杭州乘云数字技术有限公司，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字、图片或者观点的，应注明“来源：《可观测性成熟度模型白皮书》”。违反上述声明者，将追究其相关法律责任。

本声明未涉及的问题参见国家有关法律法规，当本声明与国家法律法规冲突时，以国家法律法规为准。

免责声明

报告中部分图表在标注有数据来源的情况下，版权归属原数据所有公司。本白皮书取得数据的途径来源于厂商调研、用户调研、第三方购买、国家机构、公开资料。如不同意引用，请作者来电或来函联系，我们协调给予处理（或删除）。

报告有偿提供给限定客户，应限于客户内部使用，仅供客户在开展相关工作过程中参考。如客户引用报告内容进行对外使用，所产生的误解和诉讼由客户自行负责，不承担责任。

指导单位

稳定性保障实验室

编写单位

北京爱分析科技有限公司 龙蜥社区 国网上海市电力公司信息通信公司 杭州乘云数字技术有限公司

■ 目录

一、引言	04
二、为什么需要可观测性成熟度模型	05
三、可观测性成熟度模型介绍	07
Level 1: 监控 (Monitoring)	09
Level 2: 基础可观测性 (Basic Observability)	11
Level 3: 因果可观测性 (Causal Observability)	14
Level 4: 主动可观测性 (Proactive Observability)	19
Level 5: 业务可观测性 (Business Observability)	23
四、总结	26

一 引言



莫听监控繁杂声

何妨观测且徐行

智能诊断快胜马

一键运维定乾坤

—— 引用龙蜥社区品文（毛文安）的诗

21 世纪,以数字技术为代表的第四次工业革命正在加速改变世界,数字化浪潮对各行各业成席卷之势,网络化、信息化和智能化的深度融合引领着生产模式和组织方式的变革。数字化已经不是一个企业、一个行业的使命,而是全行业、全社会的共同发展趋势。如何用数据为企业赋能,如何利用数字技术实现企业业务的转型、创新和增长,已经成为当下全球企业所面临的重要课题。

数字化正在重新定义企业的未来导向,这与企业的业务模式、业务体系及客户体验息息相关,也为持续提升企业竞争力提供了核心动力。而云计算已经逐渐成为企业数字化转型的最佳选择,尤其是在 2020 年疫情爆发的背景之下,企业上云这一进程被按下了加速键。

云计算时代下,企业的应用交付链路越来越复杂,云原生、微服务、大型分布式等新技术给企业带来竞争力的同时,也带来了全新的挑战,“云深不可见”难题突显。这些高度动态化、分布式的云原生技术与以往截然不同,这导致复杂性变得一发不可收拾。这些复杂性已经超出了现代 IT 团队的管理能力极限,并且还在不断扩大。若想解决这些复杂的挑战、并随时了解瞬息万变的环境中所发生的一切,需要全新的技术出现,“可观测性 (Observability)” 应运而生。

可观测性是当今 IT 领域最热门的话题之一, Gartner 将其列为 “2023 年度企业十大重要战略技术趋势” 之一, 并指出可观测性可以帮助企业实现数据价值最大化、加速企业数字化转型。2021 年, 中国信通院开始了可观测性系列标准的制定工作, 并成功推动了中国通信行业标准的立项。尤其是近年来云原生的广泛普及, “可观测性” 逐渐取代 “监控” 成为了企业 IT 建设与运营不可或缺的核心能力。可观测性作为一种技术或方法, 具有广阔的发展空间, 除了 IT 运维领域, 还可以在许多其他领域发挥作用并取得突破, 为社会发展带来积极影响。

二 为什么需要可观测性成熟度模型

自 2018 年，云原生计算基金会（Cloud Native Computing Foundation，CNCF）正式将可观测性引入 IT 领域以来，可观测性市场迅猛发展，涌现出一大批可观测性解决方案，企业也在寻求不同的方式打造可观测性能力。然而比较棘手的是，传统的监控厂商与新生的可观测性厂商，均使用了相同的术语与概念，这导致客户对于可观测性的定义变得模糊，甚至很难区分出哪些是真正的可观测性方案。

可观测性能力的成长，并不是简单的工具堆砌

随着软件系统的复杂性不断增加，以及对数字化体验的高质量需求日益增强，可观测性工具的增多成为了必然趋势。根据 Enterprise Strategy Group (ESG) 的一项调查，超过 63% 的企业组织拥有超过 10 种以上的工具，但即使拥有这么多工具、故障排查依然面临着困难。

ESG Report: 用于采集数据的可观测工具数量统计

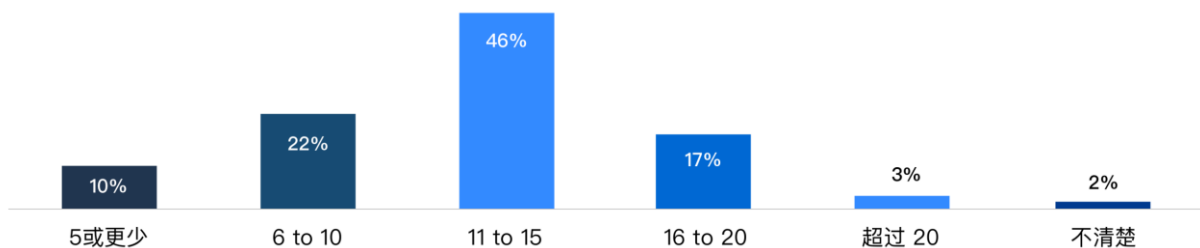


图 1: Enterprise Strategy Group. echTarget, (ESG)- Observability from Code to Cloud , 2022 年 2 月

各不相同的点式工具或方案组合在一起，反而会放大孤岛效应，这些负面影响会蔓延到每一个环节，使得团队被迫忙于处理各种局部问题或孤岛噪音。由于缺乏联系纽带，团队只能将截然不同的数据模型强行整合在一起，这不仅费时费力，还容易出错。

在测试环境或生产环境采用孤岛式的可观测，会影响到 DevOps 或 SRE 团队“测试前移”工作的速度和质量。对基础设施和平台运营者而言，在多重云或混合云平台上使用多种工具会导致可观测能力存在盲区。一旦团队接收到未覆盖区域的警报和征兆，其他团队就可能会面临“翻墙而过”的问题和指责。因此可

观测性能力的成长，并不能简单的依赖工具堆砌。

建立成熟度模型，帮助企业明确发展目标

随着动态云、容器、微服务和无服务器架构的趋势发展，以及需要维护企业原有的遗留系统的需求，对观测性更高级能力的需求日益增强。在这样的背景下，设计一套观测性成熟度模型变得非常必要。

基于对生产环境实际问题的丰富处理经验、与不同行业客户的深入交流、对最新技术的持续研究，以及与 Gartner 等领先机构的对话，我们共同创建了观测性成熟度模型。我们希望通过制作这个观测性成熟度模型，帮助企业确定在观测性道路上的位置，并为前进方向提供指引。

观测性成熟度模型能够为企业提供一种系统性的方法来评估、改进和提升其观测性体系建设。它可以帮助组织更有针对性地发展观测能力、优化资源分配并持续改进。通过合理应用该模型，企业可以更好地应对现代软件系统复杂性带来的挑战，实现更出色的用户体验，提高系统可靠性，并在竞争激烈的市场中取得优势。

三 可观测性成熟度模型介绍

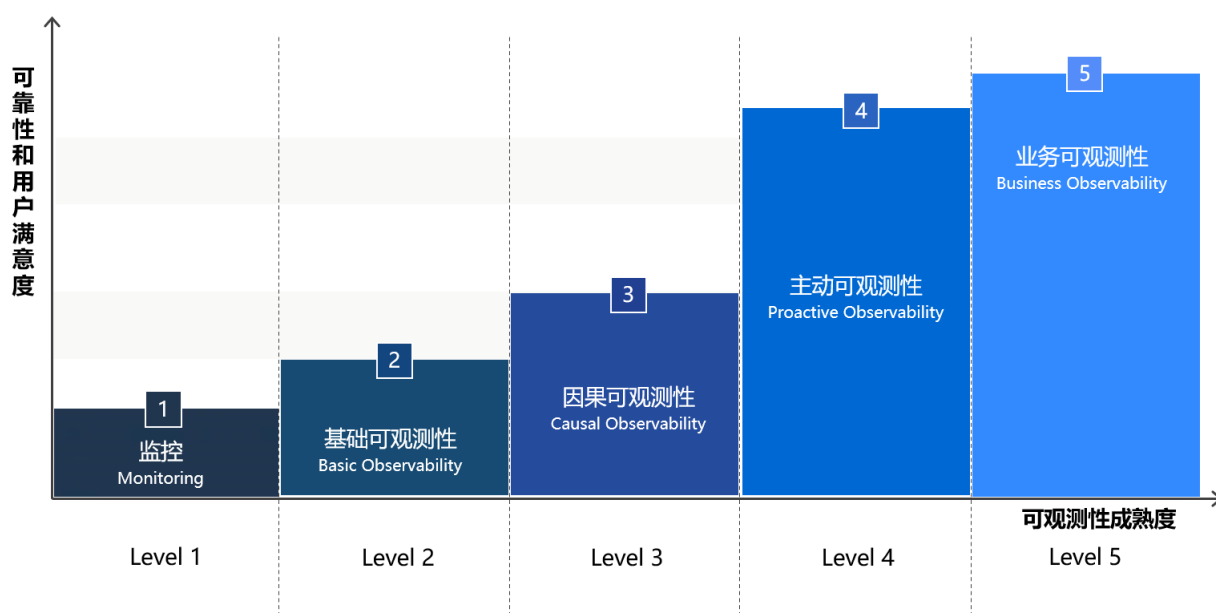


图 2: 可观测性成熟度模型图

本次设计的可观测性成熟度模型，是一种用于衡量和评估企业软件系统内部可观测性的框架或方法，同
时也是一种用于反馈企业可观测性体系建设成熟度水平的框架或方法。

该模型设计了五个级别，分别是：

- Level 1 —— 监控 (Monitoring)
- Level 2 —— 基础可观测性 (Basic Observability)
- Level 3 —— 因果可观测性 (Causal Observability)
- Level 4 —— 主动可观测性 (Proactive Observability)
- Level 5 —— 业务可观测性 (Business Observability)

可观测性成熟度模型的每个级别，都必须建立在前一级别已经建立的基础之上，不能凭空构建，每个级别新增的能力，都应该有助于实现更深度的可观测性能力。

级别的提升不是渐进式的，而是明显的跨越式提升（类似量子跃迁）。尽管我们可以通过改进流程、修修补补，在一个级别之内稍微改善结果，但若想实现级别的实质性提升，需要实质性地增强多项里程碑式能力，企业为了级别的提升甚至有可能要求重构现有的可观测架构。

下面对可观测性成熟度模型各级别的目标与功能做简要概括：

级别	目标	功能
Level 1 监控	确定系统组件是否按预期正常工作	<ul style="list-style-type: none"> · 组件健康状态监控 · 触发警报 · 出现问题时发出通知，但无法提供有关问题确切性质的详细信息
Level 2 基础可观测性	确定系统为什么不工作	<ul style="list-style-type: none"> · 采集可观测三大支柱数据 · 了解系统内部状态 · 基于三大支柱数据，手动根因分析，找到何处出错（定界，技术性问题根源）
Level 3 因果可观测性	找到问题的根本性原因（RootCause），并确定它的影响面、避免再次发生	<ul style="list-style-type: none"> · 引入网络、拓扑数据，构建更全面的系统内部理解 · 真正实现跨越全栈的监控，搞清楚系统内部的关系脉络 · 通过拓扑，为可观测数据提供锚点 · 构建空间级地图，自动捕捉绘制每一条水平、垂直连接关系 · 跟踪实体在时间、空间轴上的变化，丰富上下文背景信息，构建因果关系 · 手动根因定位，找到为何出错（定位，根本性问题根源） · 加速“Know、Triage、Understand”过程，极大压缩问题发现与定位的时间
Level 4 主动可观测性	自动化的找到问题根本性原因（Automatic RCA），自动化的响应处置，智能化的预测预防、阻止异常风险发展成问题故障	<ul style="list-style-type: none"> · 引入现代性AIOps分析引擎 · 将AI/ML与Level 3数据相结合，构建面向全栈的运维分析大脑 · 自动化根因定位，找到何处出错、为何出错（定界、定位） · 自动化问题响应，找到问题根源、并启动自动处置降低问题影响面 · 自动化问题预警，提前发现异常、发出警告 · 设想：构建超模态现代AIOps，综合预测AI、因果AI、生成式AI
Level 5 业务可观测性	确定对业务的影响，如何降低成本、增加业务营收，提升转化率、辅助商业决策	<ul style="list-style-type: none"> · 提供业务视角的端到端视图，深入洞察业务流程识别业务流程瓶颈 · 构建业务指标体系，例如销售量、转化率、用户留存等 · 收集分析业务数据，基于事实做出决策，更好地优化运营和战略 · 预测业务走向趋势，辅助业务决策 · 提供可能影响成本（FinOps）、财务收益和其他业务收益的决策信息 · 基于主动式可观测能力，自动化业务可观测性的问题分析与处置

表 1: 可观测性成熟度模型表

Level 1: 监控 (Monitoring)

目标：确定系统组件是否按预期正常工作

监控 (Monitoring)，是指对系统、进程、活动或环境的持续观察、度量和记录，以便获取实时或定期的信息和数据。通常跟踪某个系统组件的特定参数，以确保系统组件的状态保持在可接受的范围内，一旦超出预设范围，监控器会触发告警。传统监控大多是专门的单向工具、聚焦在某一个性能领域，通常包括应用性能监控 (APM)、基础设施监控 (ITIM)、网络性能监控 (NPM)、API 监控等。

在可观测性成熟度模型中，监控是其中一个关键的层级，通常被认为是成熟度模型中的第一个阶段。在这个阶段，企业开始建立基本的监控能力，监控级的目标之一是设置实时警报，以便在系统出现问题或达到预定阈值时能够及时通知运维人员，这有助于迅速采取行动以防止问题扩大。企业组织收集各种关键性能指标，将收集到的指标数据可视化也是一个重要目标。通过仪表板和图表，运维人员可以更容易地理解系统的状态和性能趋势。

在 Level1 阶段，被监控的各组件之间几乎没有任何的相关性，此级别的主要目标是了解系统组件是否正常工作。尽管在监控级不会进行深入的性能分析，但会开始对基本的性能问题进行分析，以确保系统在某些情况下不会受到显著影响。总之，监控级的主要目标是建立起最基本的监控能力，以确保系统的基本稳定性和可用性。

汇总：

下表概述了 Level 1 阶段的关键功能：

Level 1：监控 Monitoring	
了解系统组件的可用性或关键指标的状态	
输入 (Input)： 组件级指标，或事件	输出 (Output)： 警报，通知，看板
获得： 基本信息，例如组件的健康状况是否正常工作 出现问题时发出警报、通知 指标监控看板	

表 2: Level 1 总结

Level1 阶段的监控，通常为企业提供各个组件的健康状况，关注事先定义好的指标或数据，根据经验定义告警策略。这种监控方式往往是被动的，只有在特定事件或条件达到时才会触发警报。然而，这种被动性可能会导致忽略系统内部的复杂交互或潜在问题。它只告诉我们某些东西出错了，但没有解释问题的根本原因，也没有告诉我们问题最初发生的时间或背景。当问题出现时，监控可能只提供有关问题的表面信息，无法提供更多的上下文信息和相关数据。

在 Level1 阶段，由于可分析的数据有限，想要找到根因或影响面非常困难。调查问题的根源一般需要较长的周期，一个问题的出现经常可能导致整个监控体系处于“红盘”状态，各层的监控信息彼此孤立，相互割裂，难以建立起数据之间的关联。因此，需要从 Level1 升级到 Level2 来获得更深入的信息，从而提供更全面的洞察力。

Level 2: 基础可观测性 (Basic Observability)

目标: 确定系统为什么不工作

IBM 对可观测性的定义: 通常是指基于对复杂系统外部输出的了解, 能够了解其内部状态或状况的程度。系统越可观测, 定位问题根本原因的过程就越快速越准确, 而无需进行额外的测试或编码。

为保证复杂动态的系统可靠运行, 我们不仅需要知道系统组件是否正常运行, 还需要了解它为什么不运行。当出现问题时, 我们希望遵循“5W1H”的原则了解问题详情:

Who	When	Where	What	Why	How
谁	在什么时间	在什么地方	发生了什么事情	因为什么原因	我该怎么办

在监控方案中, 通常会预置仪表盘或阈值规则, 旨在提醒我们未来可能会遇到的性能问题。但是, 这些仪表盘或阈值规则依赖于一个关键性的假设, 即我们能够在问题发生之前预测将会遇到的问题类型。然而, 这种方法并不能提供足够的信息, 无法回答 5W1H 的问题。在云原生环境中, 这种类型的监控并不适用, 因为云原生环境是动态的、复杂的、多变的。这意味着我们无法事先预知可能会出现什么样的问题。在可观测性方案中, 我们可以根据更完整、更深入的可观测性数据, 灵活地探索正在发生的事情, 并快速找出可能无法预料的问题的根本原因。

可观测性能够为这些问题提供答案。

可观测性三大支柱

在 Level 2 阶段, 可观测性通过关注三种关键类型的遥测数据来提供系统洞察力: “链路”、“指标”、“日志”, 可观测性可以从这三类数据了解系统内部发生的情况。

Traces 链路数据是常规的监控工具不能采集的数据要素, 在可观测性体系中占据着重要作用。

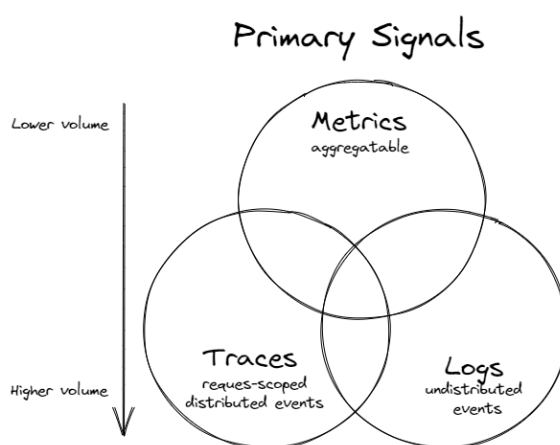


图 3: 可观测性三大支柱 (来源: CNCF 可观测性技术白皮书)

可观测性三大支柱的具体定义如下：

指标	帮助我们了解服务性能或状态的度量值 例如，著名的四大黄金信号：延迟、流量、错误率、饱和度
日志	系统中发生的相关事件，帮助我们了解系统在给定时间点的行为 例如，事务、警告、错误、带时间戳的记录
链路	详细的全链路快照显示数据如何端到端的流经应用程序，有助于排查性能问题 可以在代码级了解性能问题

Level 2 相较于 Level 1 的数据具有更大的广度和深度。然而，将这三类数据采集汇聚，汇总到一个平台是可观测性的核心。可观测性的这三大支柱来自于微服务、应用程序、数据库等 IT 组件，旨在提供对系统行为的整体视角。每个支柱都提供不同类型的信息，如上表所示。

可观测性统一平台

区别于传统监控的一大特点，可观测性强调数据的统一性，旨在通过构建一个统一的平台来实现三大支柱数据的集中汇聚与数据处理，从而打破单点工具的限制。统一平台的目标是将各种可观测性工具整合在一个集中的界面，从而使组织能够更高效地管理和维护其应用程序和系统。通过可观测性统一平台，团队可以更快地识别问题、优化性能，并提供更稳定、可靠的服务。这种集成方法有助于提高团队的协作效率，减少信息孤立，并为整个组织带来更好的业务结果。

汇总：

下表概述了 Level 2 阶段的关键功能：

Level 2: 可观测性	
采集链路、指标、日志三大支柱数据，了解系统内部状态	
输入 (Input) : 【Level 1】 + 链路、指标、日志	输出 (Output) : 【Level 1】 + 图表、火焰图、日志等可视化
<p>收获:</p> <ul style="list-style-type: none"> 从更多数据源中收集到更多的数据 通过全链路捕捉到交易级链路数据 构建更多的关键性指标，尤其是应用层指标 了解服务之间的连接关系，理清整个流程的全链路 对系统提供更广、更广深、更全面的了解 能够更好的支撑问题排查与诊断 除已知故障类型之外，还能够发现很多未知故障 	

表 3: Level 2 总结

在 Level 2 阶段，我们仍然需要通过手工关联这些数据来推断事件的可疑原因，这种方法通常需要复杂的跨系统手动查询。在 Level 2 中，尚未开发出一套自动化方法来统一和关联来自各种工具汇聚的孤立数据，因此，要准确定位问题的根本原因仍然需要大量的人力和时间。

因此，我们需要理解可观测性数据之间的关系，为 IT 环境中的数据孤岛提供上下文。当出现问题时，我们可以将上下文数据与自动化相结合，以帮助快速确定问题的根因，而无需手动遍历不相关的数据孤岛。这将引导我们进入 Level 3，即“因果可观测性”。在这个阶段，我们能够更加深入地理解事件之间的因果关系，实现根因分析的自动化，从而更高效地解决问题。

Level 3: 因果可观测性 (Causal Observability)

目标: 找到问题的根本性原因, 并确定它的影响面、避免再次发生

在实际的 IT 运维工作中, 可观测性的核心价值在于辅助问题的排查和诊断。通过分析数据, 它可以帮助我们定位到问题的原因, 甚至是找到问题的根本性原因 (RootCause)。因此, 从“因果关系”的理念出发设计一套可观测性体系, 可以更深入、更全面的理解系统的运行和行为, 能够理解系统中事件和变化之间的前因后果。通过分析这种因果关系, 可以最终找出问题的根本性原因。我们将这套可观测性体系形象的称之为“因果可观测性 (Causal Observability)”, 这个体系能够提供更高级别的洞察力, 帮助我们更快地发现问题, 更准确地解决问题, 从而提升整个系统的稳定性和可靠性。

因果可观测性, 强调寻找因果关系

因果可观测性 (Causal Observability), 是指通过收集、分析和解析数据, 以理解系统内部事件和变化之间的因果关系, 从而更深入地洞察系统的运行和行为。这一概念强调了在数据分析中寻找因果关系, 并将这些关系转化为对系统的洞察, 从而支持决策、问题排查和系统优化。

因此我们不难发现, Level2 强调数据, Level3 强调关系。

因果可观测性与基础观测性有所不同, 基础观测性关注的是收集、分析数据以理解系统的状态和行为, 而因果可观测性更加强调数据与数据、实体与实体、事件与事件或者它们相互之间的联系。在构建因果可观测性时, 常常涉及数据收集、关系收集、数据处理、关系处理、因果推断等步骤, 以揭示事件发生的前因后果。这种理解有助于更好地预测、解释、优化和管理系统, 特别是在面对复杂性、不确定性和变化性时。

根据大量项目经验积累统计, 系统故障的根源主要来自三个方面:

- 新版本部署
- 配置变更
- 基础设施可用性

因此, 在调查故障根因时, 我们需要搞清楚问题出现的时间环境、空间环境, 是什么变化导致了问题出现、以及问题如何在整个堆栈空间中传播, 这些堆栈之间的关系如何随着时间的推移而变化。

综上所述，为了解决这些问题，需要引入新的能力：网络数据、拓扑数据、时间、空间地图、自动化关联等。这些能力可以帮助我们更全面地理解系统的运行，并迅速而准确地定位问题的根本原因。

可观测五大支柱（观测五件套）

为了建立因果可观测性，需要补充更多类型的数据要素：网络、拓扑

网络 网络空间中实体之间相互的通信性能（例如容器之间的 TCP 连接数）

拓扑 系统中各实体对象相互之间的连接关系（例如根据链路相关数据绘制的服务拓扑）

在可观测性领域，网络数据（Flows）具有重要的价值。网络数据是指云网络空间中实体相互通信的信息，包括数据包、连接、协议、源/目标地址等内容。网络实体包括但不限于主机、进程、容器、Pod、服务等。通过收集和分析网络流量的元数据，可以提供有关系统内部运行和通信的深入见解，从而支持问题排查、性能优化和安全分析等方面的工作。

目前，基于 eBPF 技术采集云原生网络通信数据已经成为一种流行，业界部分领先厂商已经实现了规模商业化落地。

拓扑信息（Topology）指的是系统中各个组件、容器、服务、节点之间的关系和连接方式。拓扑的价值在于它能够提供系统的高级视图，帮助我们理解不同组件之间的依赖关系、通信路径和层次结构。通过拓扑信息，我们能够更好地把握整个系统的结构，从而更准确地分析和解决问题。

至此，我们建立了链路、指标、日志、拓扑、网络 五大关键可观测性数据要素（俗称“观测五件套”），我们将会以拓扑为中心，驱动流转多维度遥测数据、并自动集成到统一数据结构中。数据质量决定模型分析的上限，高质量的原生数据与原生关系，会为分析引擎提供高保真、原生性数据材料。

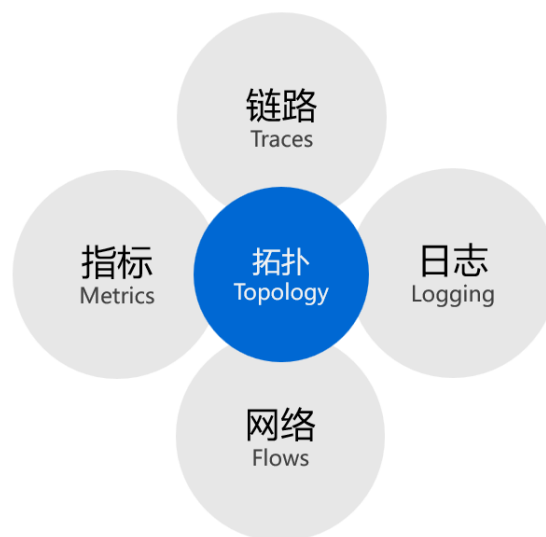


图 4：观测五件套

拓扑，为数据提供锚点



通过在拓扑结构内部分析数据，可以识别出原始数据中隐藏的模式和关系。在因果关系确定的过程中使用拓扑，可以显著提高其准确性和效果。

—— Gartner® Market Guide for AIOps Platforms, May 2022

拓扑信息在可观测性数据中扮演着一种定位和上下文的角色，帮助人们更好地理解数据所涉及的组件、服务、资源以及它们之间的关系。具体来说，拓扑信息可以看作是一个系统的结构图，展示了系统内部各个元素之间的连接和依赖关系。这种结构图可以是物理上的（如网络拓扑、主机之间的连接），也可以是逻辑上的（如服务之间的依赖关系、数据流动路径）。通过了解系统的拓扑，我们可以将可观测数据与特定的组件或服务联系起来，从而更准确地定位问题、分析数据，并理解数据在系统中的流动和影响。

拓扑信息相当于数据的上下文，它提供了一种框架，帮助你在数据中找到关联，将数据点连接到特定的系统元素上。这种关联和连接使得你可以更加深入地分析问题，更准确地做出决策，并能够更迅速地响应问题。因此，拓扑为可观测性数据提供了锚点，使得数据不再是孤立的点，而是融入了整个系统的运行背景中。

时间，追踪变化

对于大多数公司来说，仅仅添加拓扑本身不足以提供因果可观测性。尤其是在当今充满微服务、频繁部署、云资源和容器不断变化的动态环境中，拓扑信息的变化是非常迅速的。我们的系统堆栈可能在问题第一次出现时与现在的完全不同。因此，为了确立因果可观测性，我们需要引入一个至关重要的维度：时间。

为了深入了解现代 IT 环境的动态行为并获取实现因果可观测性所需的上下文。随着时间的推移，捕获拓扑信息的变化，并将其与可观测性数据进行关联，以跟踪整个堆栈的变化。当出现问题时，我们可以回溯到问题开始的确切时间点，并查看是什么变化导致了这个问题。通过这种时间维度的关联，我们能够更准确地定位问题的根本原因，实现对问题的全面分析和解决。

空间地图，可观测性能力的集大成者

空间地图，是可观测性能力的集大成者，综合体现可观测性的技术水平。

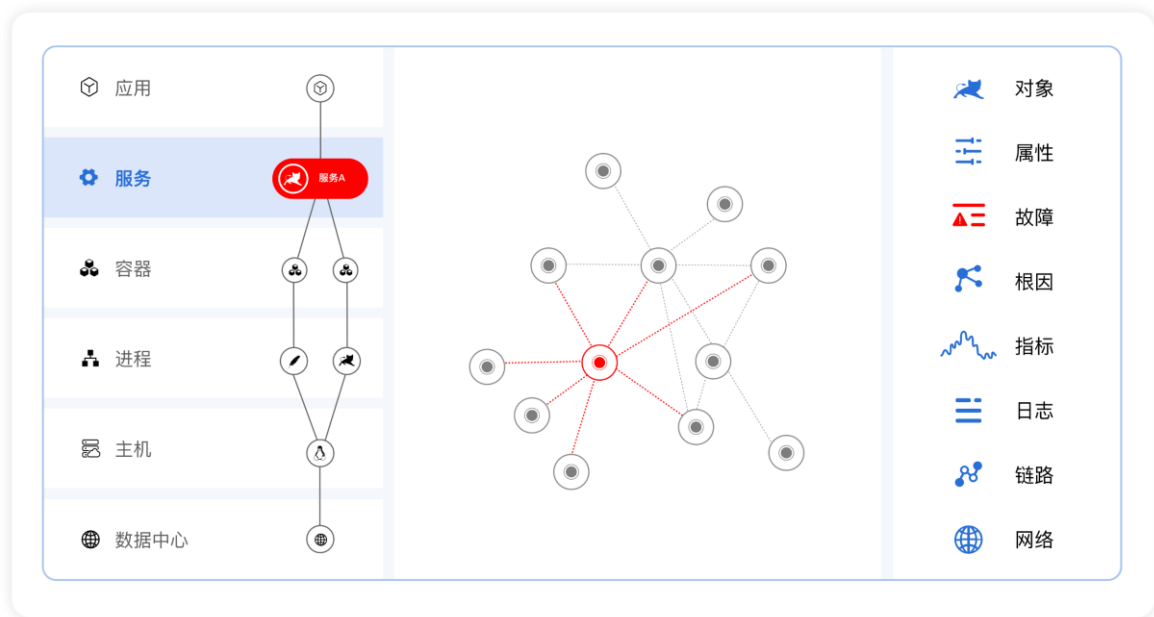


图 5: 空间地图示例

空间地图是拓扑的升维，提供 IT 环境中所有元素的关系映射，空间地图是一张三维的元素连接拓扑，涵盖水平的实体关系拓扑，垂直的依赖关系拓扑。空间地图结合了组件之间的逻辑依赖性、物理邻近性和其他关系，以提供人类可读的可视化和可操作的关系数据。

- **水平拓扑:** 在相同类型的元素之间建立的连接关系地图，如进程到进程、服务到服务、主机到主机
- **垂直拓扑:** 在不同类型的元素之间建立的连接关系地图，如数据中心到主机、主机到进程、进程到服务、服务到应用程序

通过技术实现水平层、垂直层的空间地图，自动化、实时性的绘制，将可观测性数据与空间地图的实体关联，拉动时间轴，展示随时间变化的空间拓扑、关联数据，提供时间旅行、允许我们能够比较变化前后的系统状态，是可观测性能力的集中式成果体现。

汇总:

下表概述了 Level 3 阶段的关键功能:

Level 3:因果可观测性	
通过拓扑为遥测数据（指标、链路、流量、日志）提供上下文，随着时间的推移关联所有数据，追踪变化如何在整个堆栈中传播	
输入 (Input) : 【Level1】+ 【Level2】 + 网络 + 拓扑 + 时间	输出 (Output) : 【Level1】+ 【Level2】 + 空间拓扑 + 数据关联 + 时序变化
收获: 丰富网络通信数据，加强云网络空间性能监控 强化拓扑关键性，为可观测数据提供锚点 构建自动化空间地图，提供所有堆栈的三维空间关系，将内部系统彻底白盒化 构建自动化因果关系，加速根因识别定位	

表 4: Level 3 总结

如 Gartner 所说，拓扑可以极大地提高因果判定的准确性和有效性，Level 3 对空间地图的引入是一次重大的进步。然而，统一来自不同孤岛的数据，构建空间地图都会面临数据规范化、关联性和质量等方面带来的挑战，需要大量的人工成本。特别是在不太现代化的环境中，大规模收集和操作高质量的拓扑数据是很困难的。

Level 3 阶段，数据的生成速度、数量、种类通常非常之大，如果不能友好处理、只会带来更大的噪音和分析难度。我们希望更自动化、智能化的利用好 Level 3 的这些数据和关系，这种更深层次的能力需要演进到 Level 4。

Level 4: 主动可观测性 (Proactive Observability)

目标: 自动化输出问题根源、自动问题响应, 智能预测、主动预防

Level 4 主动可观测性, 这是一种更高级的可观测性方法, 它的主要目标是通过自动化和智能化的方法来实现更深入更准确的洞察力, 将传统的被动式运维转变为主动式运维。这一层次的典型特征是引入“现代 AIOps”, 将 人工智能 (AI) 和机器学习 (ML) 技术融入到可观测性体系中, 为用户提供内生型的人工智能分析。在这一阶段中, 更加强调分析结果和答案, 而不仅仅关注原始数据和分析过程。主动可观测性希望将分析结果直接呈现给用户, 帮助用户更迅速地做出决策和采取行动。

关注结果 (Outcome) , 而非输入 (Input)



我们去面包店购买面包, 作为食客我们真正关注的是面包本身的质量和口感, 我们不会过分执着于店家采用的是何种面粉, 经过何种器材、何种烹饪的工艺。我们会根据面包的口感和质量来对店家进行评价打分。

同样的道理, 可观测性不能单独的理解为三大支柱数据, 数据只是原材料, 技术团队在实际工作过程中真正想要拿到的是结果、是原材料经过分析之后得出的答案。专注于原始数据本身, 并不能为用户提供想要的结果, 如何能够快速的把高质量结果和答案传达给技术团队, 以便快速做出决策、采取行动, 是主动可观测性需要重点考虑的问题。对于任何一家企业, 在决定采用任何一套可观测性解决方案或建设可观测性体系之前, 都应该扪心自问三个最本质的问题:

- *Know:* 在问题出现并造成影响前后, 我能够在多快的时间内得到通知?
- *Triage:* 我能够多么轻松和迅速地对问题进行分类, 了解影响?
- *Understand:* 我如何找到潜在的原因以快速解决问题?

现代 AIOps, 智能运维新范式



现代技术运营需要智能和自动化, 必须能够利用这些解决方案实现根本原因分析 (RCA) 和事件补救计划的自动化。在监控和可观察性的背景下, AIOps 需要无缝集成到整个 ITOM 工具链中。

—— Forrester Wave™: 智能运维, 2020 年第 4 季度

现代 AIOps，也被称为“内生 AIOps”或“因果 AIOps”，是一种区别于传统 AIOps 的技术路径。它建立在可观测性系统之上，利用因果关系和故障树模型进行分析。现代 AIOps 解决方案是为动态云环境和敏捷软件开发而设计的，强调高度自动化、标准化的将 AI 分析价值交付给使用者，不需要花费高昂的人力成本、工具成本，不需要耗费长周期的项目建设、数据清洗，不需要甲方费时费力的充当协调者调动各方资源。现代 AIOps 强调为云原生新场景服务，为大规模微服务分布式软件系统服务，现代 AIOps 使用的是渐进的故障树分析，是基于拓扑驱动的。



图 6: 传统 AIOps 与现代 AIOps 的对比

构建基于拓扑驱动的现代 AIOps

将可观测性与 AI 相结合，可以实时生成精确、连续、可操作的洞察力，这与传统 AIOps 方法使用概率模型来推断系统状态形成了鲜明对比。

Level 3 建立的因果关系与空间地图，为我们打造“现代 AIOps”提供了可能。现代 AIOps 是建立在 Level 3 的核心能力基础上，并引入了模式识别、异常检测、自动故障分析（Automatic RCA）等先进能力。因果可观测性是主动可观测性的必要基础，时序拓扑和空间地图为现代 AIOps 分析提供了基本框架。

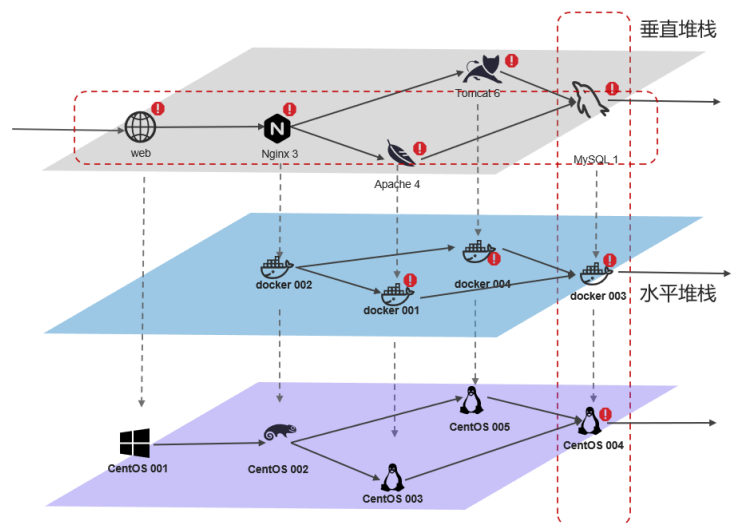


图 7: 构建基于拓扑驱动的现代 AIOps 分析示意图

真正现代的 AIOps 解决方案应该包括强大的拓扑映射功能，借助强大的拓扑映射，实时获得关于所有

基础架构、流程和服务依赖关系的全面可视化,从而更好地理解系统的运行情况和交互关系。“现代 AIOps”依托空间地图、高保真数据来进行故障树分析,故障树能显示给定警报的所有垂直和水平方向的拓扑依赖关系,能够自动、准确地确定技术性异常的问题根源。

自动化和智能化是根本所在

企业无论是选择自行开发,还是购买多套工具组装拼瓶,或是投资于商业化平台,都需要花费时间、金钱、人力、物力。对企业、客户而言,价值导向和交付速度要比在这个瞬息万变的多重云世界里找到成功之路更为重要。

若想具备面向动态多重云环境、以超出客户期望和业务目标的速度提升的可观测能力,需要采用一种截然不同的方式。如果总是在手工插装和配置、孤岛化数据剖析以及其他不该做的事情上浪费精力,妨碍团队的工作进展,最终将会影响企业战略目标的实现。自动化、智能化手段不可或缺。

自动化和智能化是转变团队工作方式的根本所在,可以迅速、高效地实现企业级的可观测能力提升。通过构建主动可观测性,可以帮助团队更快地发现问题,甚至完全预防问题的发生。AI/ML 算法模型,有助于团队了解服务或组件从什么时候开始偏离正常行为,并在出现故障之前采取措施解决问题。这种方法可以大大提高系统的稳定性、可靠性和性能,从而为企业提供更好的用户体验和业务成果。想提升可观测能力,企业组织必须从根本上改变他们工作的方式,从而加快创新、与日新月异的技术栈保持同步、降低跨团队的风险。

云自动化,未来可期

主动可观测性的另一个目标,是最大程度的减少团队的手动工作量,实现自动化的运维响应。现代 AIOps 提供的高精度分析,为构建答案驱动的自动化响应引擎铺平了道路。自动化响应引擎,使用交互式无/低代码编辑器创建工作流或将其配置为代码,使其能够根据计划或事件自动执行事件响应。这种自动化响应引擎有助于组织实现主动预防、高效运营、快速修复、强大保护和业务加速。

云自动化用例,包括但不限于:

- *针对性通知和协作: 将合适的团队链接起来,并为他们提供实时答案*
- *闭环修复: 自动修复问题和漏洞*
- *资源弹性控制: 基于监控运行数据建立服务画像,通过 AI 实现自动弹性扩缩角色,自动扩展调整资源负载分布,大幅缩减成本*

在 Level 4 阶段,我们应该关注更高效且无事故的 IT 运维,可以提供更好的客户体验。为了实现这些目标,需要设置 AIOps 来跨越数据孤岛,并从整个环境获取数据。

汇总:

下表概述了 Level 4 阶段的关键功能:

Level 4: 基于 AIOps 实现主动可观测性	
使用 AIOps 对海量数据进行分类, 并识别最重要的模式和有影响力的事件, 以便团队可以将时间集中在重要的事情上	
输入 (Input) 【Level 1-3】 + 现代AIOps	输出 (Output) 【Level 1-3】 + Automatic RCA + 云自动化 + 预测 + 预防
<p>获得:</p> <ul style="list-style-type: none">借助现代性AIOps分析引擎, 无需配置的配置操作、即可享受人工智能运维的价值将AI/ML与Level 3数据相结合, 构建面向全栈的分析大脑自动根因定位, 找到何处出错、为何出错 (定界、定位, Automatic RCA)找到问题根源、并启动自动处置, 降低问题影响面构建基于同根因的自动化告警降噪, 自动压缩告警数据提前发现异常、发出警告	

表 5: Level 4 总结

Level 4, 目前是 IT 技术领域中最高的可观测性成熟度级别。其想象空间巨大, 随着当前大语言模型的火热发展, 我们完全可以期待更有想象力的主动式可观测能力的出现。这种新颖的能力将能够更好地应对动态的系统环境, 提供更精准的洞察, 使我们的运维更加高效, 而不是受限于传统方法的局限。

Level 5: 业务可观测性 (Business Observability)

目标: 业务影响是什么? 如何降低成本, 提升业务转化, 增强竞争优势

业务可观测性 (Business Observability), 是指在一个组织或企业的业务层面上, 通过监测、分析和理解数据, 以获得对业务运行情况、用户体验和业务指标的深入洞察力的能力。业务可观测性关注的是业务过程、用户旅程和客户交互等方面的可视化和理解。业务可观测性的目标是帮助组织更好地理解业务的健康状况、用户行为和市场趋势, 以便更好地做出决策、优化业务流程, 并提供更好的用户体验。

观测升维, IT 驱动业务



到 2026 年, 70%成功应用了可观测性的企业机构, 将能够缩短决策延迟, 帮助目标业务或 IT 流程建立竞争优势。使用可观测性是指, 以高度协调和整合的方式在业务职能部门、应用和运维 (I&O) 团队中应用可观测的数据, 尽可能缩短行动与响应之间的延迟, 实现业务决策的主动规划。

——Gartner 《2023 年度十大重要战略技术趋势》

正如 Gartner 描述, 可观测性不只是应用在 IT 领域, 还可以应用在业务分析领域。业务可观测性正在兴起, 以满足企业内部数据驱动决策的需求。理想情况下, IT 数据可以为业务方面的决策提供信息。

IT 的宗旨是为业务部门提供服务, 帮助业务部门实现目标。在很多公司, IT 存在的理由是支持业务目标。在可观测性的成长进阶设计中, Level5 业务可观测性与 Level4 没有很强的继承关系。将业务可观测性列为 Level 5 , 是为了建立“以业务为导向”的可观测性体系, 让可观测性服务于企业战略, 让可观测性的价值向前。在任何企业, 业务事件的优先级要高于任何 IT 事件, 业务指标要高于任何 IT 指标。将技术可观测与业务可观测二者拉通, 是市面上几乎所有解决方案的技术瓶颈, 也是可观测价值体现的亮点。

为了衡量服务质量, IT 团队通常监视各种 IT 指标, 但这些指标与业务 KPI 之间仅仅是间接相关, 通常会导致 IT 团队工作优先级错位、协作效率低下, 严重时可能公司失去商机。通过将业务指标与 IT 指标联系起来, IT 团队可以直接跟踪业务部门的核心目标, 直接了解 IT 服务质量对业务的影响。传统上, 业务分析师和 IT 团队的领域并不容易相交。但是, 随着可观测性的出现与进步, IT 团队在业务分析桌上占有重要地位。

业务可观测性的典型用例

业务流程可视化: 将应用程序中不同组件和服务之间的关系可视化, 以帮助理解业务流程, 并识别潜在

的瓶颈和优化空间。

用户旅程分析：追踪用户在业务使用中的旅程和行为，包括点击路径、交互和停留时间，以获得关于用户体验的洞察。

业务指标监测：定义并监测关键业务指标（KPIs），如销售量、转化率等，以实时了解业务健康状态。

转化率漏斗分析：定义业务转化漏斗，捕捉用户行为和交互、收集行为数据，分析用户在转化漏斗的流动情况、识别转化率和跳出率，发现瓶颈。

趋势分析与预测：基于历史数据和趋势，进行趋势分析并预测未来的业务和性能趋势。

数据驱动决策：通过可观测性收集的数据，可以做出基于事实的决策，减少主观判断，有助于更明智地制定业务战略。

构建业务地图，拉通 IT 与 Business

基于业务视角，建立一套业务地图是业务可观测性的典型能力特性。业务地图是一种将业务流程和 IT 元素相结合可视化的方法，以帮助企业更好地理解业务的整体架构和关系。将可观测性应用于建立业务地图可以提供更深入的洞察，使我们能够实时监测业务的健康状况、性能和用户体验。

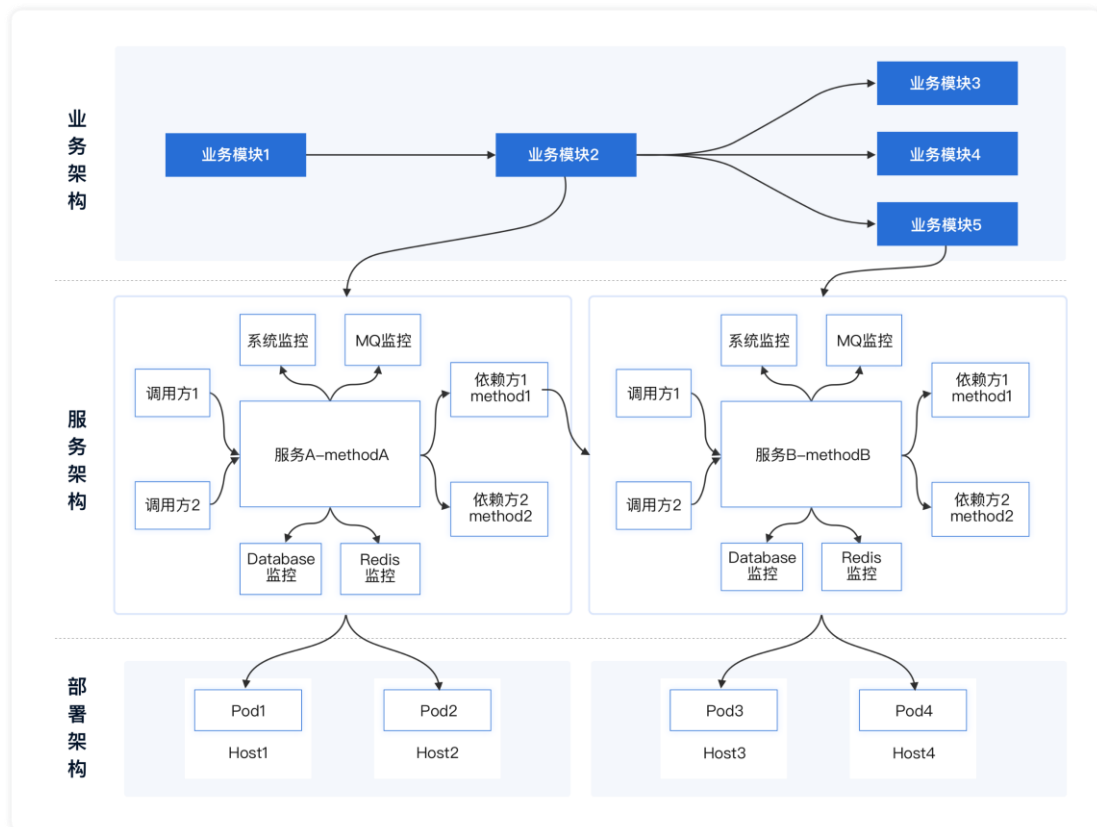


图 8: 业务地图示例

下表概述了 Level 5 阶段的关键功能:

Level 5:业务可观测性	
提供实时业务可观测性的精确分析，辅助数据驱动的决策并改进业务流程和成果	
输入 (Input) : 【Level 1-4】 + 业务数据	输出 (Output) : 【Level 1-4】 + 商业转化 + 客户画像 + 商业决策
获得: 提供业务视角的端到端视图，深入洞察业务流程识别业务流程瓶颈 构建业务指标体系，例如销售量、转化率、用户留存等 收集分析业务数据，基于事实做出决策，更好地优化运营和战略 预测业务走向趋势，辅助业务决策 提供可能影响成本 (FinOps)、财务收益和其他业务收益的决策信息 基于主动式可观测能力，自动化业务可观测性的问题分析与处置	

表6: Level 5 总结

四 总结

可观测能力的发展是一个持续演进的过程，随着技术、工具和需求的不断变化，它会逐步地适应和扩展。每个可观测性级别都有不同的目标、输入、输出和能力，我们会持续发现每个级别的典型共性，但自动化和智能化是转变团队工作方式的根本所在，可以迅速、高效地实现企业级的可观测能力提升，自动化与智能化水平是可观测性成熟度模型的一个关键评估维度。

在可观测性成熟度模型中，每个级别都建立在前一级别基础之上，如果在没有全面数据基础的情况下应用新级别的功能，可能会事倍功半。例如，如果算法给出了错误的根因，自我修复系统试图纠正错误的问题，可能进一步破坏系统。如果我们在数据不足或质量差的数据上应用 AIOps 分析，可能会因为算法学到错误的内容而导致智能运维朝错误的方向发展。

综合上述描述，我们对成熟度模型概括如下：

	Level 1 监控	Level 2 基础可观测性	Level 3 因果可观测性	Level 4 主动可观测性	Level 5 业务可观测性
可观测性目标					
确保各个组件是否按预期正常工作	●	●	●	●	●
确定系统不工作的原因		●	●	●	●
查找事件的原因并确定其对整个系统的影响			●	●	●
自动化输出问题根源、自动问题响应，智能预测、主动预防				●	●
业务影响是什么？如何降低成本，提升业务转化，增强竞争优势					●
输入 (Input)					
事件，组件级指标	●	●	●	●	●
链路，指标，日志		●	●	●	●
网络，拓扑，时间			●	●	●
现代 AIOps，自动化				●	●
业务数据，营销数据					●
输出 (Output)					
告警和通知	●	●	●	●	●
全面的仪表盘		●	●	●	●
空间地图			●	●	●
了解变化的原因和结果			●	●	●
自动化根因分析				●	●
自动化影响分析				●	●
智能告警降噪				●	●
预测和预防				●	●
云自动化				●	●
商业分析					●
商业决策					●

表 7: 可观测性成熟度模型总结

可观测性成熟度模型旨在帮助组织评估其在可观测性方面的发展水平，并提供指导和框架，以实现更高水平的可观测性。其目的主要包括以下几点：

- 帮助组织了解当前的成熟度水平，确定其在可观测性方面的优势和薄弱点
- 指导成熟度建设，制定针对性的战略计划，明确目标、里程碑和改进方向
- 了解监控、可观测、AIOps 之间的关联与差异

总之，可观测性成熟度模型是一种非常实用的工具，帮助组织评估、改进和发展其可观测性能力。通过这种能力，组织可以进行自我评估，还可以引导组织朝着更高水平的可观测性发展。通过该模型明确的步骤，我们可以提高组织内的可观测性，从而为客户提供更可靠和更具有弹性的系统或程序。

成熟度级别越高，IT 系统会变得更加弹性和可靠。我们将能够更快地解决问题的根因，了解变更、故障对业务的影响，并最终为客户提供更好的体验。借助可观测性成熟度模型，组织可以明确发展的路线，使其能够全面把握系统和应用程序的状态和性能，及时做出反应并解决问题，实现对业务的可持续监测和优化。

可观测性技术日新月异，最后，我们希望大家一起思考关于可观测性领域的几个问题：

1. 可观测性，在未来能否完全替代掉监控
2. 能否轻松快速的实现可观测性成熟度级别跃迁，少走弯路
3. 现代 AIOps，未来能否完全替代掉传统 AIOps
4. 现代 AIOps 分析结果的自动化输出，能否加速“答案”驱动故障自愈商业落地
5. 大语言模型对 IT 运维会带来多大的冲击

编写单位简介：

稳定性保障实验室

稳定性保障实验室（原混沌工程实验室），由中国信通院牵头成立于 2021 年，以保障企业云上系统稳定性、提升服务连续性、促进业务高质量发展为目标，构建了针对稳定性建设者、稳定性赋能者以及云服务稳定运行能力的稳定性保障标准体系，为我国系统稳定性保障能力建设起到了重要推动作用。

爱分析

爱分析，是一家专注于数字化市场的研究咨询机构，为企业用户、厂商和投资机构提供专业、客观、可靠的第三方研究与咨询服务，助力决策者洞察数字化趋势，拥抱数字化机会，引领中国企业数字化转型升级。

龙蜥社区

龙蜥社区（OpenAnolis）是一个面向国际的 Linux 服务器操作系统开源根社区。社区理事会由阿里云、统信软件、龙芯、Arm、Intel 等 24 家企业共同组成，有超过 500 家来自芯片厂商、软件厂商、整机厂商、操作系统厂商等覆盖操作系统全产业链的合作伙伴参与生态共建。

国网上海市电力公司信息通信公司

国网上海市电力公司信息通信公司，成立于 2010 年 1 月，主要负责信息通信系统的建设、运维、检修、技术改造、应急抢修和国家电网公司上海数据中心的建设、运行和管理工作。

杭州乘云数字技术有限公司

杭州乘云数字技术有限公司，成立于 2017 年 10 月，国家高新技术企业，是一家专注于云观测、云运维的 IT 公司，拥有多项可观测领域核心发明专利。