可观察性

初学者指南

深入了解您的系统、
服务和应用程序真
正在做什么

splunk>
turn data into doing™

可观测性被称为一切，从流行的技术流行语到一个“类固醇监测”的必备条件。事实更加复杂，尤其是考虑到现代基础设施的复杂性增加，并且，毫无疑问，需要在堆栈和系统中进行更高、更深和更好地监控。

要求运维可见性的团队已经扩展到系统管理员和 IT 运营分析师之外，甚至开发人员也更加了解如何获得更好的客户体验。为了有效地做到这一点，所有角色都需要在其整个架构中具有可见性，从第三方应用程序和服务到他们自己的应用程序和服务，以修复并最终防止问题。当这种能力成为可观察性的前提时，它不仅使可见性变得更容易，使洞察力更强，并为更具战略性的计划留出更多时间，而且对现场可靠性工程 (SRE) 的整体成功也至关重要。这在发布代码的开发人员和维护受代码影响的基础设施的操作人员之间提供了一座桥梁。最重要的是，它将一些监控工作转移到了开发上。

在本指南中，我们将定义什么是可观察性，以及实现它需要什么。我们还将提供一些可观察性的例子，并为帮助您的组织实现可观察性的解决方案提供指导。

目录


可见性
反馈
指标
检测
异常跟踪
可控制性
事件
运维智能
监控
日志
外部化它的状态
AIDevOps
跟踪
数字废物
可用性

可观察性

第 1 章

可观察性 - 它是什么和不是什么

简介

建立反馈

简单地说，可观察性就是利用系统和应用程序来收集指标和日志。它构建应用程序的想法是有人会观看它们。它来自系统控制理论，这是反馈系统的基础，通过可观察性，可以衡量系统内部状态可以从其外部输出 1 (一种数字输出) 的知识中推断出的程度。将它视为系统的一个属性 - 另一个属性，例如功能性、性能或可测试性。

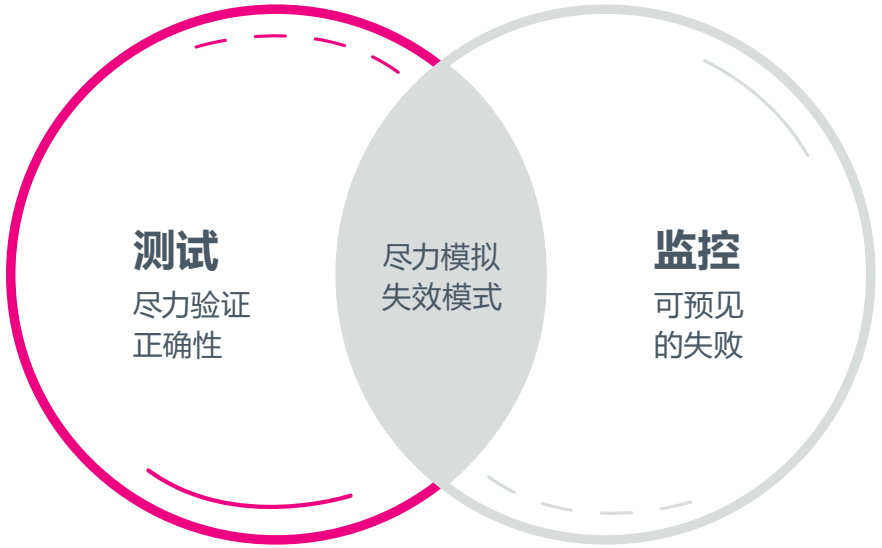
> "您可以使用各种工具对系统进行监控。但如果系统无法很好地体现其状态，您就无法弄清楚系统到底出了什么问题，进而就会陷入困境。" [2]

1. "Observability," 维基百科，2018 年。
2. Ernest Mueller, "Monitoring and Observability," agileadmin.com，2018 年 2 月。

可观察性和监控

由于监控和可观察性经常被混淆或互换，所以对二者进行比较有助于区分和定义它们。

监控	可观察性
告诉你系统运行是否正常	允许你查询系统运行不正常的原因
一系列有关系统的指标和日志记录	传播该系统的相关信息
以故障为中心	理解系统行为，无论是否停机
“**运维方式**”/你采取的措施	“**运维目标**”/你具备的条件
我**对你进行监控**	你**让自己**可以被观察到



可观察性即文化

可观察性不能代替监控；它们是互补的。但是如果没有一种可观察性文化，几乎不可能进行有效的监控。仅有工具还远远不够，也没有什么东西能神奇地"给您"可观察性。

可观察性的价值

- 规划与开发
- 解决问题
- 推动更有用的事故审查
- 提高正常运行时间和性能

作为一种文化，可观察性是一个团队或公司重视检查和理解系统、它们的工作量和它们的行为的能力的程度。具有强大可观察性文化的公司通常有可观察性团队，尽管它们可能没有这样命名。

> "如果可观性是一种文化价值，那么，想要的结果就会随之而来。"
>
> —**Andi Mann,** Splunk 首席技术倡导者

第 2 章

可观察性路线图

可观察性的支柱

在更加清晰地了解什么是可观察性后，下一步就是实现它。
以下三个支柱对于实现可观察性至关重要：

事件

随着时间推移发生的离散事件的不可变记录

指标

一些专用的数字，用于描述在一定时间间隔内测量的特定过程或活动

跟踪

一些专用的数据，用于显示哪一行代码未能在单个用户级别更好地了解已发生的事件

现代事件处理技术

有三种技术用于处理事件，最终目标是实现共享见解、协作响应、数据支持的 IT 和智能操作。

收集所有相关数据

这可以跨堆栈、技术和所有环境实现完全可见性：

- 云原生
- 传统、内部、整体等
- 混合环境

去除垃圾邮件

从噪音中分离出有价值的信号

添加上下文

确定解决方案的优先级，以确保服务的可用性，提供业务详细信息并增强对 ITSI 服务的见解

AI 和 ML 的作用

对于正在收集的数据，无论是数量、速度还是种类，人类都根本无法进行管理。可观察性允许提出问题，并让系统进行自我管理，使用人工智能 (AI) 和机器学习 (ML) 进行复杂的分析。

学习算法可以了解您的服务和应用程序过去的运行状况，以预测未来会发生什么。数据将使您能够将 AI 的一个子集 - ML 应用于您收集的历史和实时数据，并使用它来帮助预测高可能性、潜在的未来事件，并真正利用 AI 的力量来实现预测。

由于 AI 与开发运维工具和系统的融合，随着时间的推移，进行这种类型的分析将变得更加容易，提供持续和更深入的见解，并在 IT 中实现更加敏捷和高效的状态。

复杂的事件分析

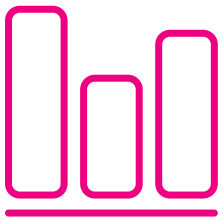
事件分析的进步实现了以下目标：

- 通过多元异常检测减少事件混乱和误报
- 自动隐藏重复事件以关注相关事件
- 通过筛选、标记和排序，轻松筛选海量事件。
- 丰富和增加事件的内容，使其具有信息性和可操作性

> "管理事故，而不是事件。"

重要指标

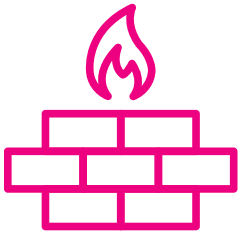
包括 Gartner、Forrester、IDC 和 Computing UK 在内的分析公司都开发了自己的"重要指标"。 以下是我们发现对实现完全可观察性至关重要的可观察指标和事件列表。



指标

常见的指标来源包括:

- 系统指标 (CPU、内存、磁盘)
- 基础设施指标 (AWS CloudWatch)
- Web 跟踪脚本 (Google Analytics)
- 应用程序代理 (APM, 错误跟踪)
- 业务指标 (收入、客户注册、退换货率、购物车放弃)



事件

事件有三种形式 - 纯文本、结构化和二进制。常见事件来源包括:

- 系统和服务器日志 (系统日志、日志)
- 防火墙和入侵检测系统日志
- 社交媒体源 (Twitter 等)
- 应用程序、平台和服务器日志 (log4j、log4net、Apache、MySQL、AWS)

收集可观察性和监控数据

好消息是存在如此多的数据；面临的挑战是将所有数据整合在一起。下面列出了多年来发展起来的数据源类型 - 所有这些对于实现可观察性都很重要。

现有来源

- 网络流量数据
- 虚拟服务器 – VC 日志、ESXi 日志等
- 云服务 - AWS 数据源，例如 EC2、EMR、S3 等
- Docker – 记录驱动程序、系统日志、应用程序日志等
- 容器和 MSA – 容器和微服务日志、容器指标和事件等
- 第三方服务 – SaaS、FaaS、无服务器等
- 控制系统 - vCenter、Swarm、Kubennetes 等
- 开发自动化 – Jenkins、Sonarcube
- 基础设施编排 – Chef、Puppet、Ansible
- 用于安全分析的信号 – DLP、设备遥测、元数据
- 来自移动设备的信号 - 产品采用、用户和客户、功能采用等
- 业务分析指标 - 应用程序数据、HTTP 事件、SFA/CRM
- 来自社交情绪分析的信号 - 分析一段时间内的推文
- 客户体验分析 - 应用程序日志、业务流程日志、通话详细记录等
- 服务智能分析 - 急诊就诊、治疗等待时间、处方等。
- 消息总线和中间件

更新的来源

- collectd – 用于收集指标的守护程序
- statsd – 用于监听统计数据的守护程序
- ßuentd – 用于统一日志数据收集的守护程序
- 来自现代服务的信号，例如 Splunk
- Zipkin、Jaeger – 首选的后端分布式跟踪系统
- 语义日志 – 创造新的信号

相对于可观察性，这些守护程序会将指标发送到定义的位置，这将创建和定义重要的指标，并在这些指标超出限制时采取行动。

您的代码只有在构建了支持它的分析之后才“完成”。

如果没有这种可见性，您就无法确定系统失败的原因，这会降低对关键业务问题的响应和解决时间。

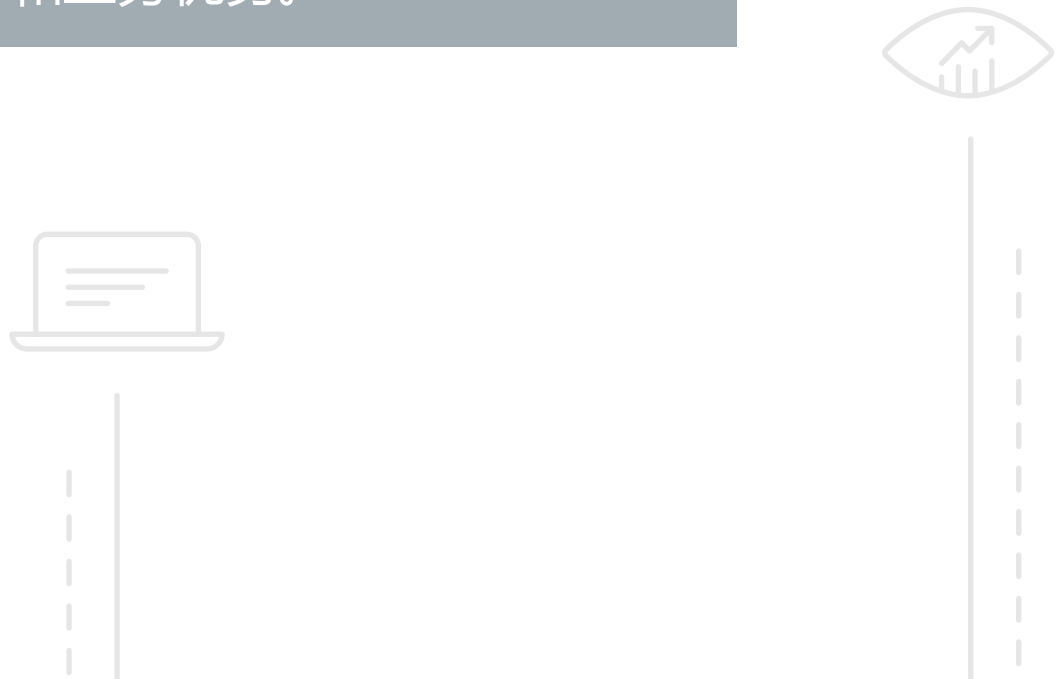
第 3 章

行动中的可观察性

简介

既然我们已经讨论了什么是可观察性，为什么它很重要，以及它所基于的指标和事件，现在让我们看看行动中的可观察性以及它可以帮助实现的 IT 和业务优势。

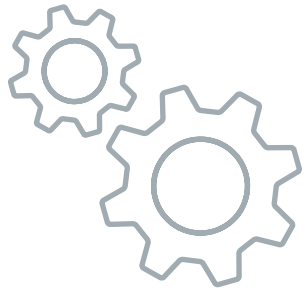
以下案例研究显示了使用 Splunk 软件可视化和关联事件和指标，以及对数据源中出现的问题进行故障排除和补救的实际客户结果。现代 IT 组织在运营和开发日志记录这两个关键领域都体验到了巨大的好处。



运营

Cox Automotive – 为了更好地了解其内部和在线拍卖平台的运营情况，以便能够实时发现、排除和预防问题，Cox Automotive 部署了 Splunk IT 服务智能 (ITSI)、Splunk Enterprise 和 Splunk Cloud。该公司看到了以下好处:

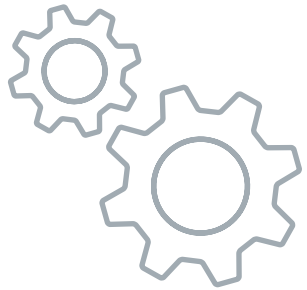
- 同播可靠性的提高增加了利润
- 显著提高了平均识别时间 (MTTI)
- 拍卖事件数量减少了 90%
- 支持更主动的设备更换: KPI 预测停机并提供实时降级监控



运营

ENGIE – 该能源交易平台需要一个集中、实时的关键交易应用运行状况视图，以加快故障排除并确保性能。自从部署 Splunk Enterprise 和 Splunk IT 服务智能版 (ITSI) 以来，该公司已经看到了以下优势：

- 关键业务服务运行情况的整体视图
- 更快地解决影响业务的问题
- 在事故分类过程中改进开发团队和基础设施团队之间的协作



运营

TransUnion – 这家金融服务公司需要建立外部客户流量和客户交易量的基准。自从采用 Splunk Enterprise、Splunk IT 服务智能 (ITSI) 和 Splunk 机器学习工具包进行企业 IT 监控以来，该公司获得了以下能力：

- 提供可靠的交易并满足客户 SLA
- 根据机器数据实时监控、预测和维护交易
- 在几分钟而不是几小时内发现事件根本原因
- 减少错误警报的数量
- 通过改进交易处理增加收入

[日志记录]

Hyatt – 这家全球酒店公司需要一个集中的解决方案来监控和解决服务器问题，并改善应用程序交付。自从实施 Splunk Enterprise 和机器学习工具包以来，Hyatt 开发团队获得了以下优势：

- 从数小时或数分钟到实时的更快平均解决时间 (MTTR)，可即时查看整个企业
- 提高开发人员的工作效率
- 通过主动监控改善客户体验

开发日志记录

Yelp – 为了确保数百万通过其网站和移动应用程序与当地企业联系的人获得良好的客户体验，Yelp 在 Splunk 数据分析平台上实现了标准化，使数百名技术和非技术用户（从网站可靠性工程师到产品经理）能够获得可操作的业务见解。自从部署 Splunk 以来，Yelp 已经看到了以下优势：

- 通过实时通知提高网站正常运行时间
- 快速可靠地向用户交付应用程序功能
- 发掘业务见解并改善客户体验
- 通过为所有用户释放数据来节省工程时间

[日志记录]

FamilySearch – 这个家谱组织需要一种方法来转向连续交付模式，管理其到 Amazon Web Services (AWS) 的全面迁移，并立即解决网站错误。自从部署 Splunk 以来，该组织已经看到了以下优势：

- 从每月发布成功迁移到每天 900 多次部署
- 能够将 12 名开发人员重新分配到更多增值任务中
- 了解 AWS 环境，以支持 AWS 迁移战略

第 4 章

可观察性选项

简介

随着对可观察性的需求和要求的增长，一些监控工具供应商也加入了这股潮流 - 大约和几年前他们使用开发运维的速度一样快。没有任何工具会“给您”可观察性。这是一个良方谬论，在研究选项时应该成为一个危险信号。

许多供应商声称拥有完全的可观察性能力，但仔细观察会发现，他们只提供了可观察性的一部分。提供部分视图只是可观察性的一个组成部分，根据定义，这是无法实现的。

专为新 IT 打造的可观察性

随着组织开始实施可观察性，人们越来越关注新的 IT - 一种具有开发运维 (即 CI/CD) 操作模式的 IT。理想的可观察性解决方案具有支持以下三大支柱的属性，这三大支柱定义了 IT 发展的新方向：

监控

集中查看所有相关的基础设施和应用程序。根据上下文检测根本原因分析，创造一种可观察性文化，以防止并最终预测问题重复出现。

协作

跨组织孤岛，与每个利益相关方共享重要数据，以管理事件解决方案并构建可重复的行动计划。

自动化

化繁为简。自动化流程以节省时间，专注于真正重要的事情，例如战略业务计划，而不仅仅是监控和故障排除。最终，协调多个流程，优化监控、根本原因分析和补救中的人工干预。

适用于新 IT 的 Splunk

适用于 IT 的 Splunk 支持团队实现从被动到主动再到预测性的 IT 发展，在问题的整个周期中提供解决方案，帮助组织创建可观察性文化，并做出数据驱动的决策。适用于 IT 的 Splunk 提供了一种闭环方法来帮助 IT 团队集中他们所有最可操作的数据，专注于最重要的见解，然后不断改进他们的监控、事件响应和事件解决策略。

通过应用从根本原因分析中获得的经验教训，IT 团队可以改进他们的系统，以避免重复相同的问题，并允许他们专注于创新。

我们的大多数客户都是从使用 Splunk 进行被动故障排除开始他们的旅程的，他们只是通过查看指标、日志和跟踪来找到问题的根本原因。这是 Splunk Enterprise 的世界，允许您索引来自许多来源的数据并搜索它。随着客户成熟度的提高，他们希望监控他们的数据，将这些数据组织到服务中，并最终预测问题和防止问题再次发生。这是 Splunk IT 服务智能 (ITSI) 的世界 - Splunk 对监控服务的回答。希望对监控过程中发现的问题采取行动的客户可以使用 Splunk 和 Virtuops，这使 Splunk 用户能够在虚拟环境中协作，尽快解决问题。

IT 创造商业价值

借助 Splunk，组织能够：

- 从他们的数字废物中发现并创造可操作的价值
- 最大化 IT 资源的价值
- 缩短决策时间，以便他们在解决 IT 问题时能够更快、更明智地采取行动
- 采取一种新的方法，通过提供及时、可信的数据驱动决策，让 IT 部门成为企业的价值创造者

结论

对可观察性进行大力宣传将获得丰厚的回报。它允许运营部对正常运行时间和性能拥有更大的自主权，并且它需要组织具有一种可观察性文化来取得成功。可观察性提供了整个系统的端到端可见性，因此您可以获得可量化的结果。这使 IT 部门能够更快地解决并最终防止问题，为战略计划留出更多时间。实现可观察性的最佳方法是与 IT 的新方向保持一致的方法，在 AI 和 ML 的帮助下，通过监控、协作和自动化来跟踪问题的周期。使用 Splunk 实现可观察性的客户已经获得了广泛的可衡量的业务成果，并使 IT 部门成为业务的价值创造者。

Splunk 基础设施见解 (SII) 是在您的 IT 基础设施中实现可观察性的第一步。

免费开始使用

20-20901-Splunk-Beginners-Guide-to-Observability-EB-106

splunk>
turn data into doing™