AIOps
基本指南

打破数据乱局并对您的
IT 运维持续进行分析

splunk>

目录

AIOps 是什么?

AIOps 是将分析和机器学习应用至大数据，以实现 IT 运营自动化并对其进行改善的做法。这些新的学习系统可以对大量的网络和机器数据进行分析，以发现有时人工操作员无法识别的模式。这些模式既可以识别现有问题的原因，又可以预测未来的影响。AIOps 的最终目标是实现常规操作的自动化，以提高问题识别的准确性和速度，进而使 IT 人员能够更有效地满足不断增长的需求。

历史与起源

"AIOps"一词由 Gartner 于 2016 年首先提出。在**《AIOps 平台市场指南》中**，Gartner 将 AIOps 平台描述为"AIOps (参见注释 1) 平台是一种软件系统，它将大数据和人工指南 (AI) 或机器学习功能结合起来，以增强和部分取代广泛的 IT 运营流程和任务，包括可用性和性能监控、事件关联和分析、IT 服务管理和自动化。"

AIOps 如今的发展情况

现如今，运维团队需要做更多的工作。旧的工具和系统似乎永远不会消亡，这是一种常见的做法，有时甚至会让人觉得可笑。然而，同样的运维团队一直承受着支持更多新项目和技术的压力，而且往往面临人手不足或减少的窘境。除此之外，系统更改频率增加和更高的吞吐量通常意味着这些监控工具生成的数据几乎无法消化。

为了应对这些挑战，AIOps：

- **可将多个来源的数据集合在一起：** 传统的 IT 运维方法、工具和解决方案通过降低数据保真度的简单方式聚合并平均分配数据（例如，可以考虑被称为"平均数的平均数"的聚合技术）。它们的设计不适用于当今万物互联的复杂 IT 环境生成数据的数量、种类和速度。AIOps 平台的一个基本原则是，它能够捕获任何类型的大型数据集，同时可保持完整的数据保真度，以便进行全面分析。分析师应该始终能够下钻到提供任何聚合结论的源数据。
- **简化数据分析：** AIOps 平台的一个重要区别是，它能够对这些大型多样的数据集进行关联。只有拥有最好的数据，才能进行最好的分析。然后，平台对这些数据应用自动分析，通过检查来自许多来源的，看似不相干的流之间的交叉，确定现有问题的原因，并预测未来的问题。
- **实现响应的自动化：** 识别和预测问题非常重要，但如果可以通知正确的人员、在发现问题后自动纠正问题，或者在理想情况下执行命令，彻底防止问题发生时，AIOps 平台就可以发挥最大的作用。常见的补救措施（如重新启动组件或清理已满磁盘）可以自动处理，这样，只有典型解决方案无法解决问题时，才需要工作人员的介入。

AIOps 的主要业务优势

AIOps 可以通过实现 IT 运维功能的自动化来增强并改进系统性能，进而为组织提供显著的业务优势。例如：

- 避免停机可以提高客户和员工的满意度和信心。
- 将以前孤立的数据源整合在一起便可以提供更完整的分析和见解。
- 加快根本原因分析和补救可以节省时间、成本和资源。
- 提升事件响应速度和一致性可以改进服务交付方式。
- 更快地发现并解决复杂问题可以提高 IT 部门支持增长的能力。
- 主动发现并防止错误可以使 IT 团队专注于价值更高的分析和优化。
- 主动响应可以提高对系统和应用程序增长的预见性，以满足未来的需求。
- 通过处理平凡的工作，为不堪重负的系统增加"松弛感"，让人员能够专注于更高层次的问题，产生更高的工作效率和更高的士气。

数据对 AIOps 至关重要

数据是任何成功自动解决方案的基础。您需要历史和实时数据来了解过去，预测未来最有可能发生的事。为了对事件进行全面了解，组织必须访问大量历史和流式数据类型，包括人工和机器生成的数据。

来自更多来源的更好的数据将产生分析算法，以便能够更好地发现人类难以隔离的相关性，从而产生可以更好地进行规划的自动化任务。例如，在大多数半现代的监控系统中，实现某种响应的自动化并不困难。但是，如果响应时间使应用程序变慢，AIOps 就会帮助确保适当的自动响应，而不仅仅是静态连接的"膝跳式"响应。如果瓶颈与容量无关，向服务添加更多容量实际上可能会使响应速度更慢。而且它肯定会在云环境中造成意外且不必要的成本。因此，拥有适当的数据来做出更全面的决定会带来更好的结果。

为了实现完全可见性，需要能够跨所有 IT 孤岛在一个位置访问所有这些数据。了解支持您的服务和应用程序的底层数据，定义用来确定运行状况和性能状态的关键性能指标 (KPI) 非常重要。随着您超越数据聚合、搜索和可视化来监控和排除 IT 故障，机器学习成为实现具预测性的分析和自动化的关键。

关键 AIOps 用例

根据 Gartner 的说法，AIOps 有五个主要用例：

1. 性能分析

2. 异常检测

3. 事件关联与分析

4. IT 服务管理

5. 自动化

1. 性能分析:

对 IT 专业人员来说，就算结合了机器学习技术，使用传统的 IT 方法分析数据仍然变得越来越困难。数据的量和种类都太多了。AIOps 可应用更复杂的技术来分析更大的数据集，以确定准确的服务级别，从而帮助解决数据量和复杂性不断增加的问题，这通常可以在性能问题出现之前防止问题的发生。

2. 异常检测:

机器学习对异常数据识别特别有效，即数据集中与历史数据差异较大，可以说明可能存在问题的事件和活动。这些异常数据称为异常事件。即使以前没有发现过问题，异常检测也可以识别问题，并且无需对每种情况进行显式警报配置。

异常检测依赖于算法。趋势算法通过将单个关键性能指标 (KPI) 的当前行为与过去行为进行比较，来对指标进行监控。如果指数差异过大，算法将发出警报。内聚算法会对一组预期行为相似的 KPI 进行查看，并会在一个或多个 KPI 行为发生变化时发出警报。这种方法比简单地监控原始指标提供的见解更加深入，可以作为指示组件和服务运行状况的晴雨表。

AIOps 可以让异常检测更加快速和有效。发现异常行为后，AIOps 就可以对相应 KPI 的实际值与机器学习模型预测值之间的差异进行监控，并检测有无明显偏差。

在复杂系统中，准确的异常检测至关重要，因为提供故障支持的 IT 专业人员无法保证总是可以快速了解故障的存在方式。

3. 事件关联与分析:

通过多个相关警告识别“事件风暴”，确定事件根本原因的能力。大多数复杂系统的现实情况是，总是会有一些元素显示出“红色”或警告状态。这是在所难免的。然而，传统 IT 工具的问题在于，它们无法提供对问题的深入分析，只是会出现警报风暴。然而，传统 IT 工具的问题在于，它们无法提供对问题的深入分析，只是会出现警报风暴。这就产生了一种叫做“警觉疲劳”的现象；团队经常会看到一个不重要的警报，以至于在该警报的确很重要时也会被忽略。

AIOps 会自动根据相似性对重要事件进行分组。可以把这种方式看作在同属一类的事件周围画一个圈，而不管它们的来源或形式如何。对类似事件进行分组可以减轻 IT 团队的负担并减少不必要的事件流量和噪声。AIOps 关注关键事件组，并可执行基于规则的操作，例如合并重复事件、禁止警报或在收到事件时关闭异常事件。这使团队能够更有效地比较信息，以确定问题的原因。

4. **IT 服务管理 (ITSM):** 通用术语，指组织中 IT 服务设计、构建、交付、支持和管理相关的所有事项。ITSM 包括向组织内的最终用户交付 IT 服务的策略、过程和程序。

AIOps 可以让 IT 专业人员将其服务作为一个整体，而不是单个组件来管理，进而为 ITSM 提供便利。然后，他们可以使用这些整体概念来定义系统阈值和自动响应，以便与他们的 ITSM 框架保持一致，帮助 IT 部门更有效地运行 。

用于 ITSM 的 AIOps 可以帮助 IT 部门从业务角度管理整个服务，而不是单独管理组件。例如，如果三台机器中的一台服务器在正常加载期间遇到问题，人们可能就会认为整体服务的风险较低，而且可以在不对用户产生任何影响的情况下对服务器进行脱机操作。相反，如果在高负载期间发生相同的事件，则可以在对任何性能过低的系统进行脱机操作前自动决定添加新的容量。

此外，用于 ITSM 的 AIOps 可以帮助：

- 在多云环境中更加一致地管理基础设施性能
- 对容量规划做出更准确的预测
- 根据预测需求自动调整容量，实现最大的存储资源可用性
- 根据历史数据和预测提高资源利用率
- 对通过复杂网络连接的设备进行管理

5. **自动化:** 传统工具通常需要从多个源手动将信息拼凑在一起，然后才能理解、排除故障并解决事故。AIOps 具有显著优势，可在完整服务中自动收集和关联多个来源的数据，可显著提升确定必要关系的速度和准确性。组织能够很好地处理数据流的关联和分析后，下一步就是要实现对异常条件的自动响应。

AIOps 方法可以在组织的 IT 运维中实现这些功能的自动化，进而采取简单的操作，否则响应人员就不得不自己执行这些操作。我们以服务器为例，在高容量期间，由于已知问题的日志记录，服务器往往每隔几周就会耗尽磁盘空间。一般情况下，响应人员的任务就是登录、检查系统行为是否正常、清理过多的日志、释放磁盘空间并确认系统是否恢复了正常的性能。这些步骤可以自动执行，这样就可以创建一个事件，并且只有在已经尝试正常响应方式并且无法对情况进行补救的情况下才会通知响应人员。这些操作范围很广，从简单的重新启动服务器或将服务器从负载均衡器池中退出，到取消最近更改或重新构建服务器（容器或其他）等更复杂的操作。

AIOps 自动化还可应用于:

- 服务器、操作系统和网络: 收集所有日志、指标、配置和消息, 以便跨多个服务器执行搜索、关联、警报和报告活动。
- 容器: 收集、搜索容器数据并将其与其他基础设施数据关联, 以改善服务上下文、监测和报告。
- 云监控: 监控云基础设施的性能、使用情况和可用性。
- 虚拟化监控: 获取有关虚拟堆栈的可视性, 快速进行事件关联并搜索跨越虚拟和物理组件的交易。
- 存储监控: 通过相应的应用性能、服务器响应时间和虚拟化开销, 可在上下文中理解您的存储系统。
- 应用监控: 确定应用程序服务级别, 并生成建议或自动响应, 以维护已定义的服务级别目标。

AIOps 和向主动 IT 的转变

AIOps 的主要优势之一是, 它能够帮助 IT 部门在事件发生前预测并预防事件, 而不是等到事件发生后才去修复。AIOps, 特别是对 IT 组织监控的所有数据应用机器学习, 旨在帮助您实现这种转变。

通过减少与检测、故障排除和解决事件相关的手动任务, 您的团队不仅可以节省时间, 而且可为系统营造出关键的"松弛感"。这种松弛感可以让你将时间花在具有更高价值的任务上, 比如提高客户服务质量。您可以通过持续维护和改进来保持并提升客户体验。

AIOps 可以对关键 IT KPI 的提升产生重大影响, 包括:

- 增加故障之间的平均时间 (MTBF)
- 减少平均检测时间 (MTTD)
- 减少平均调查时间 (MTTI)
- 减少平均解决时间 (MTTR)

使用 AIOps 实施主动式监控方法的 IT 组织看到了各种 IT 指标的显著改善, 包括:

如何开始使用 AIOps?

开始使用 AIOps 的最佳方法是增量法。与大多数新技术计划一样，计划是关键。下面是开始阶段的一些重要考虑因素。

选择鼓舞人心的示例

如果您正在为您的组织评估 AIOps 解决方案、平台和供应商，那么您将面临一项艰巨的任务。最具挑战性的问题可能不是评估过程本身，而是获得执行评估所需要的支持和领导的认可。如果您选择受益于 AIOps 的其他类似组织鼓舞人心的示例（并且有指标可以证明），你将更容易获得许可。一个好的伙伴可以帮助你做到这一点。（请参见下文中的*选择适当的合作伙伴*。）

考虑人员和流程问题

很明显，技术在 AIOps 中扮演着重要的角色，但是制定计划，来处理人员和流程问题也同样十分重要。例如，如果一个 AIOps 解决方案可以识别出一个即将发生的问题，并指定支持团队进行干预，响应人员可能会忽略警告，因为实际上没有出现任何问题。这可能会在 AIOps 解决方案有机会在运维过程中被证明之前破坏人们对它的信任。

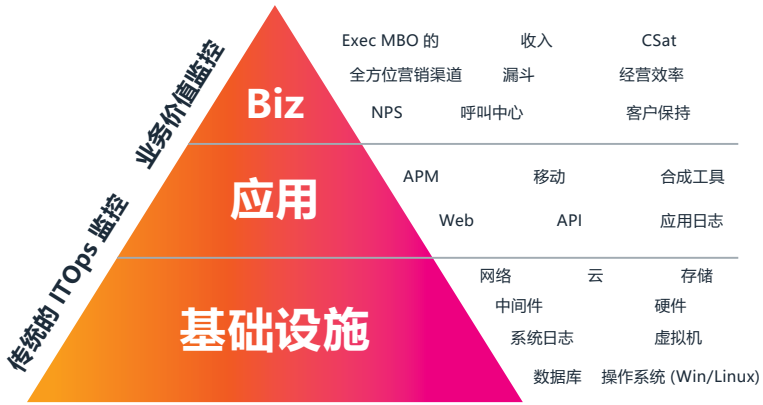
给 IT 团队一定的时间来构建、维护并改进系统也很重要。 如果您需要进行有意义的改变，就不能把这项至关重要的工作作为次要项目或入门级工作来分配。将这项任务交给你最得力的干将。将其列为优先事项，这样，其他工作就不会对其产生影响。AIOps 实践是迭代的，必须随着时间的推移而改进；这只能通过成熟和一致地关注改进来实现。

您还需要重新检查和调整之前具有多级管理批准层级的手动流程，比如重新启动服务器。这需要对技术和团队实践的信任。 建立信任需要时间。从简单的成功开始，逐渐提升对自动化文化的接受度。例如，准备构建历史报告，以显示之前的事件经过一致、简单的活动（如重启或磁盘清理）正确处理，并针对未来类似问题的此类任务主动实现自动化。通过为某些活动插入审批门，选择一个允许"自动化损害"的解决方案。随着时间的推移，这些门应该被移除，以提高速度，因为分析可以证明它在选择正确自动化任务方面的价值。

最后，在您的计划中加入一项活动，让员工放心，AIOps 的目的不是用机器人取代人。向他们展示 AIOps 如何将关键资源用于高价值活动，限制团队每天必须忍受的计划外工作。

盘活您的数据

启用 AIOps 需要访问所有类型的数据: 非结构化的机器数据和结构化的指标, 以及用于丰富的关系数据。不仅要按类型考虑数据, 还要按数据在"堆栈"中的位置考虑数据, 从基础设施开始, 向上移动到应用程序, 最后是业务应用程序。您需要每一层的数据。



这些不同的数据类型允许您跨所有孤岛构建一个整体的视角, 并对情况和数据类型采取有意义的行动。您的目标是在每个服务层识别数据源, 从基础设施 (云或传统) 开始, 向上移动到应用程序性能, 最后绑定可识别的业务结果 (如客户满意度、收入、订单数量、等待时间等) 。每个级别选择少量的源 (一个或两个) , 并首先将它们关联起来。

有效、快速地摄取和分析所有数据可能会让人望而生畏。相反, 从访问和分析原始历史机器和指标数据开始, 建立基础理解, 并使用聚类算法和分析来识别趋势和模式。原始数据最适合实时检测。然后, 您可以开始分析流数据, 考察其对这些模式的适应情况, 应用由机器学习提供技术支持的人工智能实现自动化, 最后是预测分析。

历史数据在您开始使用 AIOps 时非常有价值。如果通过分析和理解系统之前的状态开始, 就可以将了解到的情况与现在的情况进行关联, 以便得出有意义的服务水平阈值。

为了实现这一点, 组织必须接收并提供对大量历史和流式数据类型的访问。选择的数据类型 (可以是日志、指标、文本、网络和社交媒体数据) 取决于要解决的问题。例如, 您可以使用来自基础设施的指标数据来监控容量或应用程序日志, 以确保为客户提供出色的体验。

许多 AIOps 平台都会有只关注一种数据源的经历。单个数据类型的限制会限制您对系统行为的见解, 不管这些见解是来自 IT 管理员还是算法。因此, 企业应该选择那些能够从多个来源摄取和分析数据的平台。

选择适当的合作伙伴

随着 AIOps 逐渐兴起，一些供应商正在将传统的 IT 运维工具打包在一起，添加基本的 AI 功能，并将结果称为 AIOps“平台”。 但真正的 AIOps 平台不仅仅是工具的集合。重要的是，开始时就要理解这一点，因为我们选择的平台将决定成败。Gartner 建议企业“优先考虑那些允许部署数据摄取、存储和访问的供应商，而不是依赖其他 AIOps 组件。” 您需要一个能够以完全可靠的方式收集所有必要数据的平台，而不仅仅是聚合或汇总。您需要一个平台来丰富、分析和处理数据，从而得出有意义的结论和见解 (并且不需要大量的自定义工作来配置或维护) 。您需要一个可以集成适当自动化功能的平台来在正确的时间采取正确的行动，就像一个联系紧密的生态系统。

查看功能集，并查看客户案例研究和 AIOps 用例。要知道 AIOps 平台是否能满足您的需求，最简单的方法是找到可以展示类似公司如何将 AIOps 应用于其业务挑战的客户案例研究。寻找在线展示其客户，并寻求客户意见的供应商。如果 AIOps 工具或平台能够实现理想的效果，但公司无法提供证据，那么这应该是寻找其他供应商的线索。

Splunk 的 AIOps 方案为何与众不同

Splunk 可以轻松从几乎任何来源获取几乎任何类型的数据，无论是实时数据还是历史数据，然后应用高级的分析功能，如预测分析、预测和预报、事件管理和分析、聚类、自适应和统计阈值设定、异常检测、根本原因确定等等。这种独特的方法有助于增强广泛的 IT 操作和任务，并允许公司获得仅靠人工分析无法获得的价值。

差异化数据处理方法——一切从数据开始

Splunk 的 AIOps 平台是唯一一个拥有 Splunk 强大功能的"数据到一切"平台，它使客户能够将数据爆炸用作提升效率、生产力、数据分析和自动化的机会，以便在组织内部的任何位置将数据转化为行动。

如果没有正确的数据支持，即使是最好的机器学习能力也无能为力。IT 基础设施和应用程序产生的数据量的快速增长造成的复杂性增加，各种数据类型的增加，以及数据产生速度的增加，加之成本降低的推波助澜，让 IT 部门面临重重挑战，进而无法充分完成自己的工作，更不用说利用最好的转换分析。

不同的数据处理方法有的会被视为篡改功能，有的则可以实现真正的成功和转变，着实是天壤之别。作为数据到一切的平台，无论是在现场部署，还是在云端部署，Splunk 几乎可以从任何工具和系统中获取任何类型的数据，比如日志、指标、文本、网络、API，甚至是社交媒体。Splunk 可以以结构化、半结构化或非结构化的形式摄取这些数据，并通过历史或实时的方式执行所有这些操作。

想象一下，一个单个的平台将所有不同的数据统一在一起—然后想象一下 AI 和 ML 可以做什么。想象一下，团队不再被过多的警报、复杂的工具或相互割裂的视图所累，想象一下，团队在问题发生之前就提前解决了问题。

"数据到一切"平台使您能够为 AIOps 平台提供解决各种 IT 挑战所需的所有数据。任何其他 AIOps 方案都只能提供部分解决方案。

差异

- 解决方案以 AI 和 ML 为核心，灵活且可扩展
  - 结果：最多可提前 30 分钟预测服务降级
- 使用动态阈值和异常检测等 AIOps 功能简化事件管理和事件响应
  - 结果：事件噪声降低 95%
- 对基础设施、应用程序和服务进行监控和数据分析
  - 结果：可用于 IT 和业务服务的监控和服务性能运行状况视图

核心功能

- 事件管理和分析
  - 快速事件分组和关联，以控制噪声
- 阈值
  - 考虑并适应业务活动和数据中的常规模式
- 根本原因分析
  - 建立 IT 和业务环境镜像，以更快地调查和确定贡献最大的 KPI
- 异常检测
  - 从过去的行为中找出偏差，以发现异常事件
- 预测性分析
  - 预测运行状况得分并预报趋势，预防事件发生

Splunk 的优势

- 降低噪声和复杂性
  - 通过自动警报和转移简化事件检测
  - 在所有 ITOps 功能中应用人工智能和机器学习功能，以实现随组织一起成长的灵活且可扩展的解决方案
- 在影响客户之前预测中断
  - 对不同服务、应用程序和基础设施的数据使用预测性原因分析
  - 通过自适应阈值、异常检测和服务运行状况预测算法提前 30-40 分钟预测服务降级
- 360° 可视性
  - 可对不同应用程序、系统和基础设施的运行状况实现完整的可见性
  - 将任何类型的数据和性能指标组合到一个可使用的位置

总结：AIOps 时代已经来临

如果您是一名 IT 和网络专业人士，您就会反复听到这样的说法，数据是公司最重要的资产，大数据将彻底改变您的世界。机器学习和人工智能将产生变革性影响，而 AIOps 可以为 IT 部门提供一种利用其潜能的具体方式。从提高响应能力到简化复杂的运维任务，再到提高整个 IT 团队的工作效率，AIOps 是一种实用、随时可用的方法，可帮助增长和扩展 IT 运维，以应对未来挑战。也许最重要的是，AIOps 可以巩固 IT 人员作为业务增长战略推动者的角色。

了解更多信息。

有关 AIOps 的更多信息：

- **IT 运维人工智能 (AIOps)**
- **AIOps 平台市场指南**

splunk>

2020-Splunk-AIOps-Essential Guide to AIOps-117-EB-web