解决方案概述

ARUBA 网络分析引擎

加速故障排查和根本原因分析

在当今的数字世界中，网络运营人员面临着许多挑战。物联网接入的设备数量成指数级增加，而 IT 人员必须负责将这些设备接入网络并保证其安全。云的采用在网络上形成了不同的流量模式，而运营人员常常无法实现对性能的可见性。最后，工作人员的流动性意味着员工会通过多个网络访问应用程序，而每个网络又会提供不同级别的性能和安全性。

高度可用、始终在线的网络对于当今企业至关重要。然而，这些技术趋势使得这一目标难以实现，因为它们会在网络上形成更大的压力和更多故障点。

网络运营人员现在需要更好的可见性，以便在发生问题时快速解决问题。为了满足这一需求，Aruba 开发了网络分析引擎 (NAE)，它是 AOS-CX 网络操作系统的一部分。

NAE 可提供一个用于监控和排除网络故障的内置框架。它可以自动查询并分析网络事件，以实现前所未有的停机和异常可见性。利用这些数据分析，IT 人员可以实时检测问题，并分析趋势，以预测甚至避免未来的安全和性能问题。

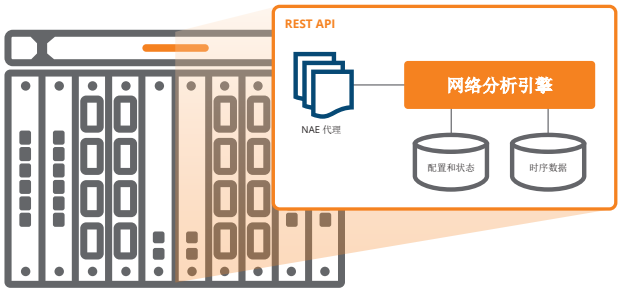
主要优势

- **速度更快，完整的可视性：**内置的时序数据库可提供事件和关联历史记录，并可实时访问全网范围内的数据分析，以帮助运营人员提供更好的体验
- **更快速的平均故障修复时间：**基于规则的实时监控和智能通知可自动与配置更改进行关联，以帮助加快例行诊断程序
- **简化管理：**与 Aruba NetEdit 和第三方工具（如 ServiceNow 和 Slack）的集成可提供智能化功能，进而将丰富的 NAE 警报集成到 IT 服务管理流程中
- **持续创新：**访问不断增长的 Aruba 精选 NAE 解决方案库以及致力于实现更多创新的专家社区

从问题到根本原因

查找网络问题的根本原因一直都会涉及许多不同的任务。首先，网络运营人员可以使用一系列 show 命令来调查网络的当前状态，或者运行探测来尝试重现问题。

如果从出现问题的那一刻起就可以进行遥测，通常还需要外部工具和人工配置，以进行正确的分析。但是这些数据通道往往未经过滤，进而造成传输和处理数据的延迟。第二，通常情况下，通过第三方监控工具对数据进行采样，而不是捕获完整的细节，从而在可见性方面带来额外的缺失。



Aruba NAE 可提供：

- 与配置变更相关联的相关历史数据
- 自动化服务影响和根本原因分析
- “始终在线”的智能监控代理
- 对所有系统信息的完整遥测
- 来自邻近基础设施的信息
- 自动诊断通知

图 1：Aruba NAE 可在交换机上本地收集高级网络分析数据

相反，NAE 可直接在每个交换机上执行智能监控，在不会产生延迟或丢失信息的情况下，为运营人员提供分布式分析能力以及全网运行健康状况的可操作视图。

通过 NAE，运营人员可以主动设置规则来监控特定的目标流量，收集数据，并将其与可触发服务警报的事件关联起来。NAE 可以通过这种方式快速深入了解问题根源，加速服务影响和根本原因分析，从而实现更快的平均故障解决时间 (MTTR)。

NAE 组件

NAE 可在 Aruba CX 6000 和 Aruba CX 8000 交换机系列等 AOS-CX 操作系统支持的平台内部运行（图 2）。它通过可以从两个关键数据库提取数据的代理来监控交换机的配置情况：

- 配置和状态数据库：可为 NAE 代理提供对配置、协议状态和网络统计数据的完整访问权限，所有这些信息均可通过 REST API 实现完全公开。
- 时序数据库：包含与配置更改相关联的相关历史数据。运营人员可通过这种方式获得围绕网络事件捕获、存档和快速访问网络状态的能力。

NAE 代理可对交换机、其相邻设备或通过网络的流量的状况进行测试，然后根据测试结果采取相应操作。

例如，由未知主机触发的 ACL 高命中数表示可能存在安全漏洞。在这种情况下，NAE 可以通过创建 Syslog 消息或生成带有分析结果的自定义报告（可以通过网页界面轻松访问）针对该问题提醒运营人员。

运营人员还可以将多项操作整合到现有工作流中，以执行更多选择性诊断或建议。这包括在发生相应问题时向 ServiceNow 等 IT 服务管理系统或 Slack 等协作工具发送通知的能力。

除了提供监视交换机状态的能力外，Web UI 还允许网络团队查看 NAE 代理、脚本和提醒并对其进行配置。

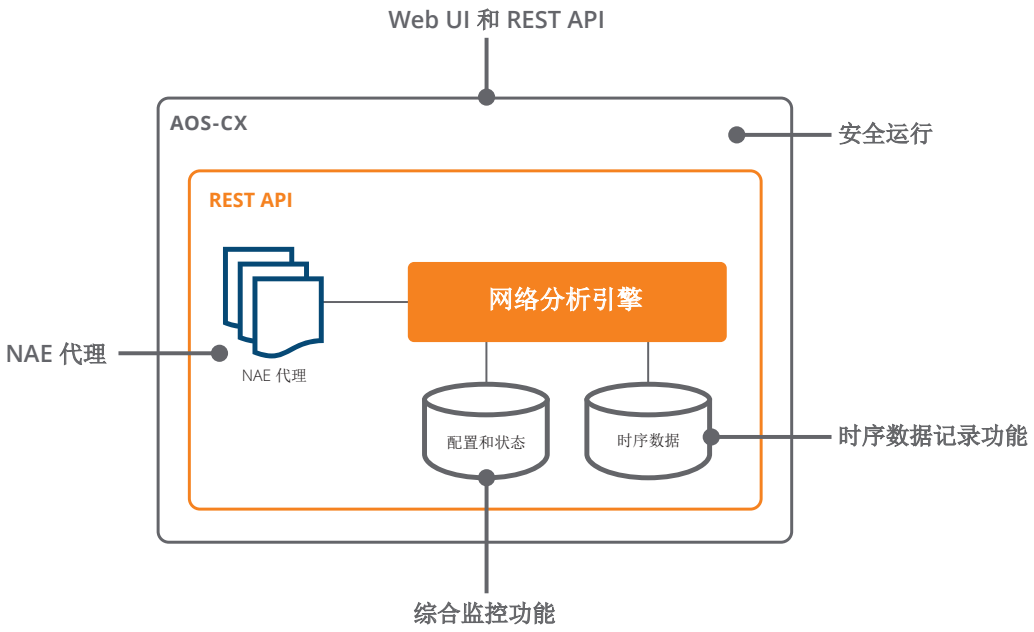


图 2：NAE 组件

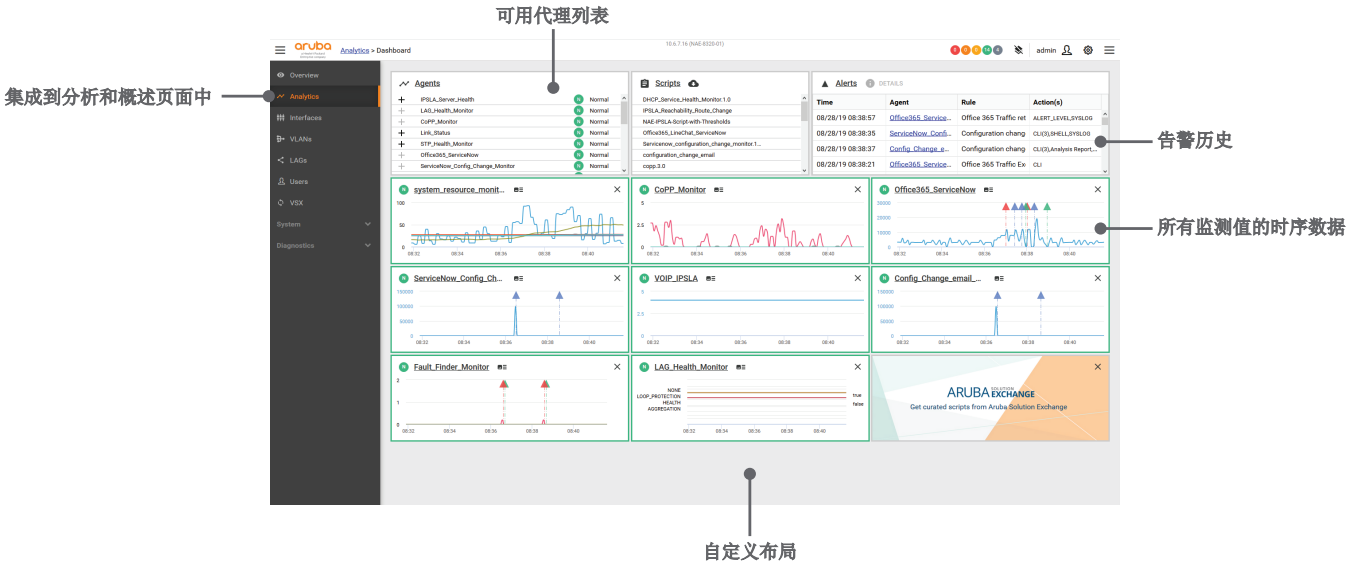


图 3：Aruba NAE 仪表板

用例

NAE 可将网络问题映射到其共同的根本原因，通过预先确定许多一阶和二阶诊断来加速故障排查常规程序，以便运营人员能够集中精力解决更多更有针对性的问题。

在更广泛的层次上，NAE 代理的用例有：

1. 系统运行状况
2. 网络分析
3. 安全
4. 应用程序可见性
5. 网络优化

系统运行状况

组织需要关于其交换机状态和性能的可靠情报。相关 NAE 代理可监控 CPU 和内存使用情况等控制面系统资源的运行状况，并随时对其进行跟踪。运营人员收到异常警报时，NAE 会在峰值时捕获并存档详细系统信息。

系统运行状况代理还可确保关键服务（如 TACACS+ 和 Syslog）的可用性。如果不可用，这些代理将执行网络诊断或采取其他适当的操作（例如带外通知）。

网络分析

NAE 可将 AOS-CX 中提供的所有网络统计数据与时序数据库进行整合，以便进行分析。这类功能的广度涵盖了从第 1 层收发器监控到第 3 层 BGP 对等体运行状况的所有方面。

凭借监控系统中几乎每个统计数据的功能，可以衍生出广泛的用例。用例示例包括：

- 收发器运行状况：通过监控收发器 TX 和 RX 功率水平，NAE 可以检测到与连接运行状况有关的几个不同的问题。如果功率水平突然变化，NAE 会将这些水平与已知的基准进行比较，并就两个收发器之间的光纤链路发生的情况提供高概率指导。
- OSPF 路由运行状况：OSPF 等路由协议对网络的运行有着巨大的影响。NAE 可为 OSPF 表中的更改提供上下文。例如，NAE 可以监控链路状态通告 (LSA) 计数器，提供系统中可用路由数的数据分析。LSA 数的突然下降可能意味着 OSPF 相邻设备不可用或不再提供正常数量的路由。这通常表示出现可达性问题，而 NAE 可提供对其根本原因的快速数据分析。

其他网络分析代理包括虚拟路由器冗余协议 (VRRP)、链路聚合 (LACP) 运行状况或生成树协议 (STP) 运行状况监控器，以及接口统计数据监控器。

安全

NAE 还可以在网络的接入层、汇聚层和核心层识别并检查通过 AOS-CX 交换机传递的错误流量。发生这种情况时，NAE 可以对流量采取相应操作，或者将其定向到安全设备，进行详细检查。

以 HVAC 系统为例，它通常只能与 HVAC 控制器进行交互。如果 NAE 发现来自这个系统的流量与源代码存储库或数据库服务器进行交互，很可能这就是一个被黑客攻击的设备。NAE 可以将此流量定向到 Aruba IntroSpect（一种用户和实体行为分析 (UEBA) 解决方案），用于完整和高强度的端点诊断。经过调查，管理员可以调整允许异常流量的策略，或者使用 Aruba ClearPass 自动对受损设备采取隔离措施。

其他安全代理包括配置更改监控器和控制平面策略 (COPP) 监控器。

应用程序可见性

NAE 还可对通过网络核心的应用程序流量提供可见性。这包括跟踪云应用程序（如 Office 365 或 Google Suite）的性能。

检测到任何性能降级时，NAE 代理就会执行强大的网络诊断。例如，如果互联网服务提供商 (ISP) 提供的服务出现性能降级，NAE 就可以进行数据分析，确定服务开始出现问题的时间，从而大大缩短进行隔离并解决根本原因所需的时间。

其他应用程序可见性代理包括用于监控队列速率是否异常的 VOIP 队列运行状况，以及用于监控请求速率并提示不匹配根本原因的 DHCP 中继统计信息。

网络优化

除了加快根本原因分析，NAE 还可以对网络上的流量进行优化。通过利用接口使用情况和应用程序性能统计信息，NAE 可以调整路由的权重，以将应用程序流量定向到不同的链路或不同的提供商。NAE 还可以监控流量比率并确保 LAG 的利用率基本相同，进而防止或纠正 LAG 不平衡的情况。此类功能可以确保为企业及其用户提供更好的服务。

与 NETEDIT 集成，提升管理简便性

NAE 可与 Aruba 的交换机配置和编排工具 NetEdit 紧密集成。IT 团队可以借助 NetEdit 顺畅协调推出端到端服务，实现快速和自动化的网络更新，并确保网络更新后的策略一致性。

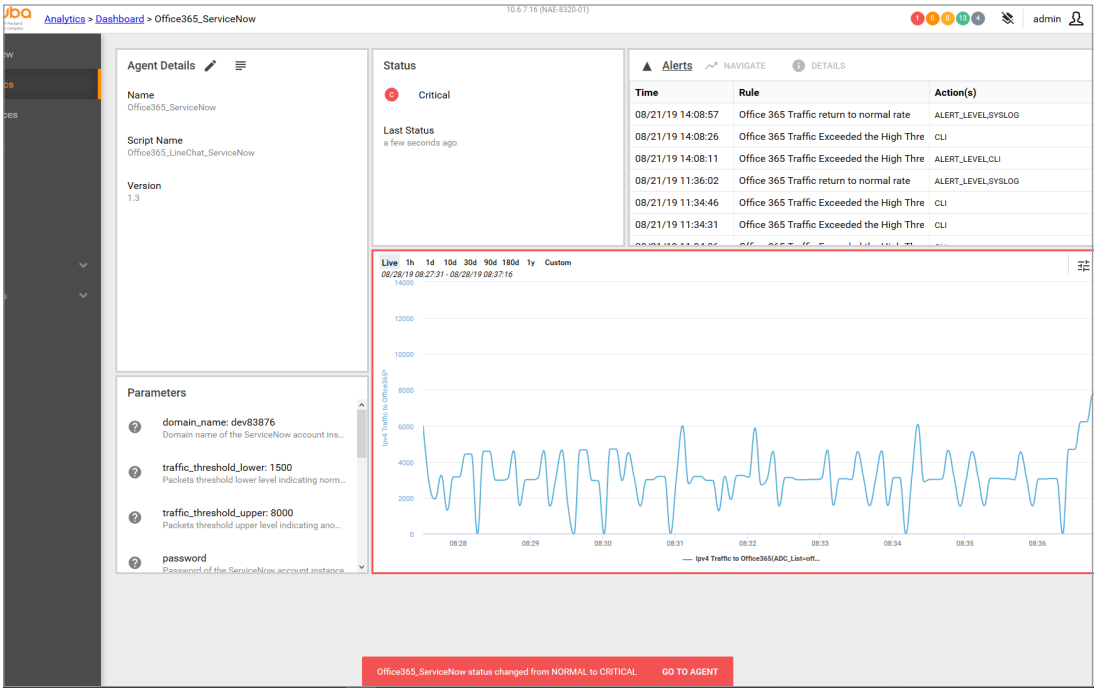


图 4：Office 365 服务降级严重警报

借助 NAE 的嵌入式分析功能，NetEdit 还可为网络运营人员提供从单个控制台监控并排除故障的强大数据分析功能。

NetEdit 可订阅 NAE 代理的状态，在发生相应问题时收集数据，并通过 Slack 或其他 ITSM 工具向运营人员提交通知。点击进入 NetEdit 后，运营人员可以立即看到受影响的设备和服务，并提供与事件发生时间相对应的完整诊断详细信息。

通过这种方式，NetEdit 和 NAE 可以显著减少通过传统方法排除问题时产生的手动数据收集和关联的工作量。它在网络上产生的负载也较少，因此在采集遥测数据的过程中不会影响性能。

社区发展

为了帮助客户充分利用 NAE，Aruba 创建了一个强大的共享代理和脚本库，以便为客户和社区提供开源许可证。这些资源均可在 Aruba Solutions Exchange 和 Github 上获得。

Aruba Airheads 社区还可为开发人员和网络工程师提供在线论坛，方便他们为其他特殊用例展开讨论、构建并分享 NAE 代理，进而实现众包开发的开发形式。

结论

IT 团队需要实现更大的网络运行状况可见性，以满足对弹性、性能和敏捷性的需求。客户可以通过 NAE 实时访问分布式全网分析，再加上不断增长的脚本库，进而实现诊断任务执行的自动化，以加快故障排查速度并改善网络运营人员的体验。

要了解更多有关 NAE 和其他交换解决方案的信息，**请访问** Aruba **网站**，以获取产品数据表、技术概述等材料。

您还可以在 Aruba Solutions Exchange 或 GitHub 上查看 Aruba CX 6000 和 Aruba CX 8000 交换机系列上提供的完整 NAE 代理库。

a Hewlett Packard Enterprise company

SO_NAE_092519 a00059004enw