事件驱动型基础架构自动化的 4 个用例

Event-Driven Ansible 是红帽® Ansible® 自动化平台中的一项功能，可帮助您主动应对 IT 环境中的事件。它可以按照规则将事件源与相应的操作连接起来。随着采用 Event-Driven Ansible 的高级功能，自动化成为维持 IT 投资回报率（ROI）和性能的任务关键型领域。

Ansible Rulebook 能够定义事件源，并使用简单的条件指令“if-this-then- that”来阐明在满足特定条件时要采取的操作。这意味着当特定事件发生时，Event-Driven Ansible 会根据设计的 Rulebook 识别出事件，并自动执行与该事件匹配的操作。此类操作可以包括各种响应，例如执行现有的 Ansible Playbook、呈报事件以作进一步调查，或者使用相关事件有效负载信息来创建或增强服务工单。

了解一下 Event-Driven Ansible 的以下 4 个用例。

1 更高效地修复 ServiceNow ITSM 事件

Event-Driven Ansible 目前已实现与适用于 ServiceNow IT 服务管理（ITSM）的红帽 Ansible 认证内容集的集成，但除此之外还可用于实现以下目标：

- 增强 ServiceNow ITSM、Ansible 自动化平台及其他系统与组件之间的闭环自动化流程。
- 使用 Event-Driven Ansible 通知服务来增强、强化和修复问题，从而帮助 IT 团队提高工作效率并减少摩擦。
- 收集与工单相关的信息，并通过其他故障排除数据来扩充事件情况，以帮助简化问题解决过程。
- 当虚拟机请求等条件超过指定的最大数量时，将服务目录订单提升到其他审批者。

2 使用红帽智能分析对红帽企业 Linux 进行故障排除

红帽智能分析是几乎所有红帽订阅中都包含的一款工具，它能够持续分析平台和应用，并且可以通过其通知服务触发事件。它还可以作为红帽企业 Linux® 中事件的事件源，如恶意软件、系统配置错误、配置偏移、违反合规性和政策等。

使用 Event-Driven Ansible 与红帽智能分析，您可以：

- 响应红帽企业 Linux 环境中的事件。
- 启动适当的 Ansible Playbook 来修复任何问题，同时创建新的 ServiceNow ITSM 事件来分析根本原因。
- 使用系统日志（systemd）和系统事件主动纠正 SELinux 违规行为。
- 利用 Event-Driven Ansible，根据来自 Performance Co-Pilot 的性能指标来修复红帽企业 Linux 上的问题。

3 利用 Microsoft Windows 和 Active Directory 丰富工单信息

Microsoft Windows 具有全面的事件记录功能，其中包括在添加、删除或更新用户帐户时产生的可能有用的信息。除了使用 Ansible 自动化平台在 Windows 主机和 Active Directory 中置备这些用户，您还可以：

- 使用 Ansible 自动化平台收集事件的有效负载，然后创建并扩充一个新的 ServiceNow ITSM 工单，同时更新配置管理数据库（CMDB）。
- 确保对事件（如防火墙错误通知）进行一致的自动化故障排除。在这种情况下，您可以指定可能需要的额外用户干预，而不是应用自动修复。
- 使用相关数据更新工单，帮助繁忙的 IT 团队缩短调查问题的时间，同时降低整体安全风险。

4 根据存储遥测数据来制定决策

将 Event-Driven Ansible 与遥测数据相集成，可为管理存储环境提供主动、高效的方法。这样您就可以：

- 在主机报告访问存储时出现问题的情况下，Event-Driven Ansible 会自动触发额外的信息收集和故障排除。
- 除了存储，还覆盖网络或存储区域网络（SAN）互连。
- 大幅缩短对关键基础架构事件的响应时间，帮助确保系统可靠性和正常运行时间。

试用 Event-Driven Ansible

开始构建您的第一个 Ansible Rulebook。

了解 Event-Driven Ansible 的实际应用

立即观看视频。

销售及技术支持

800 810 2100
400 890 2100

红帽北京办公地址

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层　邮编: 100020
8610 6533 9300

红帽官方微博　红帽官方微信

cn.redhat.com
#1015315OM_0224