# Introdução à Gestão de Eventos

O Priax possui a funcionalidade de gestão de eventos que permite que fatos relevantes do ambiente sejam direcionados às Equipes e pessoas adequadas baseado em diversas características do evento que podem influenciar em quem deve ser notificado em cada situação.

## Tipos de Eventos

O Priax possui a capacidade de detectar, classificar, filtrar e notificar os seguintes tipos de eventos do ambiente de TI:

- Eventos de Disponibilidade: Recursos que entram em situação de indisponibilidade, deixando de cumprir seu papel no ambiente de TI.
- Eventos de Capacidade: Recursos que operam em regime precário, podendo representar ineficiência ou falhas eventuais devido à sobrecarga ou falta de recursos de hardware ou má configuração.
- Eventos de Mudança: Mudanças em configurações sem prévio conhecimento.
- Logs: Logs que representam a necessidade de atenção por parte de alguma equipe de operação.

## Fluxo da Gestão de Eventos no Priax

O Priax realiza desde a detecção do evento, com agentes próprios ou integrado à ferramentas de terceiros capazes de capturar eventos nos recursos gerenciados, até a gestão pós-mortem destes eventos. Ao detectar eventos, o Priax realiza uma série de atividades até que sejam efetivamente notificados às equipes interessadas. As principais fases da gestão de eventos são:

### Monitoramento Contínuo

Os sistemas de TI são monitorados constantemente por ferramentas que coletam dados de logs, métricas, transações e outros sinais emitidos por servidores, aplicativos, redes e dispositivos.

### Detecção de Eventos Relevantes

Nem todos os eventos detectados são significativos. O processo de detecção inclui filtros para diferenciar eventos importantes (como erros críticos) de eventos rotineiros. Este processo inclui a filtragem de eventos de acordo com os parâmetros selecionados pelos usuários do Priax, além de mecanismos de detecção de falsos positivos e atenuação de pequenas oscilações normais do ambiente. Nesta fase também são realizadas os cálculos estatísticos e utilização de dados históricos para cálculo gatilhos de anormalidade com técnicas de machine learning.

### Classificação do Evento

Eventos detectados são classificados por sua criticidade (information, warning, average, critical ou down) e priorizados com base no impacto potencial no ambiente. Também são calculados os SLAs com base nos serviços impactados.

## Correlação de Eventos

O Priax utiliza **IA** e **machine learning** para correlacionar eventos aparentemente desconexos e identificar padrões, ajudando a prever problemas antes que ocorram. A correlação de eventos é o processo de identificar relações entre eventos aparentemente independentes para determinar uma causa raiz ou padrão subjacente. Em ambientes complexos, muitos eventos isolados podem ser sintomas do mesmo problema.

### Técnicas de Correlacionamento:

- **Coleta Centralizada:** Eventos são reunidos em uma plataforma central (como um SIEM ou ferramenta de monitoramento).
- **Análise Temporal:** Eventos ocorrendo em curtos períodos de tempo podem ser correlacionados.
- **Reconhecimento de Padrões:** Ferramentas usam algoritmos (ou mesmo IA) para identificar padrões comuns que indicam incidentes recorrentes.
- **Modelagem de Dependências:** Mapas de dependências entre sistemas ajudam a correlacionar eventos com base na hierarquia ou comunicação entre componentes.

## Identificação de Impactos de Eventos

Dado um evento, devidamente correlacionado e identificado sua causa-raiz, o Priax realiza a análise de impactos, identificando, baseado nas dependências presentes na CMDB, a análise de quais os recursos, aplicações e serviços afetados pelo evento, permitindo. Isso permite que se tenha imediatamente uma análise da gravidade do evento e que se ajuste o SLA do evento baseado nos impactos gerados pelo evento.

## Seleção de Responsáveis por Eventos

Com as informações de causa-raiz e impatos, é possível então definir os responsáveis por agir e mitigar as consequências do evento. Para isso o Priax possui regras que podem definir baseado em:

- Horário de ocorrência do evento
- Causa raiz e tipos de causa raiz (tipo de IC e grupos de tipo de IC)
- Impactos
- Tags
- Host e Grupos de Host

## Notificações do Evento

O Priax possui aplicativo próprio para gestão dos eventos, capaz de receber notificações em celular ou em aplicativo Windows. No entanto o Priax também é capaz de notificar usando SMS, Whatsapp,

Telegram, Microsoft Teams.

# Post-Mortem do Evento

O **processo de post-mortem de um evento** é uma prática essencial para analisar incidentes críticos ocorridos em ambientes de TI, com o objetivo de entender o que aconteceu, identificar a causa raiz e implementar ações para evitar a recorrência. Ele é parte integrante de uma cultura de aprendizado contínuo e melhoria, especialmente em equipes que seguem metodologias como **DevOps**, **SRE** (Site Reliability Engineering), ou **ITIL**.

O Priax oferece ferramentas para realização completa do processo de Post-Mortem de um evento tais como:

1. **Registro do Incidente**
   - Documentar o incidente de forma detalhada, incluindo:
     - Data e hora do início e fim.
     - Serviços ou sistemas afetados.
     - Impacto no negócio ou nos usuários.
   - Integração com Ferramentas de ITSM (ServiceNow, Jira, Helix, OTRS)
2. **Linha do Tempo do Incidente**
   - Reconstituir uma **timeline** detalhada do incidente:
     - O que aconteceu e quando.
     - Quem fez o quê.
     - Como o incidente foi detectado.
   - Ferramentas de logs e monitoramento podem ajudar a criar uma visão cronológica.
3. **Identificação da Causa Raiz**
   - Usar técnicas como:
     - **5 Porquês (5 Whys):** Perguntar repetidamente "Por quê?" até chegar à causa raiz.
     - **Análise de Árvore de Falhas:** Diagramar as falhas e suas inter-relações.
   - Diferenciar entre causas imediatas (sintomas) e causas profundas.
4. **Avaliação da Resposta ao Incidente**
   - Avaliar como a equipe respondeu:
     - O que funcionou bem (boas práticas)?
     - Onde houve falhas no processo ou demora na resolução?
   - Identificar gaps em alertas, playbooks ou habilidades da equipe.
5. **Ações Corretivas e Preventivas**
   - Propor ações concretas para evitar a repetição do problema, como:
     - Melhorias em configurações ou infraestrutura.
     - Atualizações em playbooks ou runbooks.
     - Revisão de SLAs e práticas de monitoramento.
     - Treinamentos para a equipe.
6. **Compartilhamento do Relatório**
   - Documentar o post-mortem em um relatório claro e objetivo, incluindo:
     - Descrição do incidente.
     - Linha do tempo.

    - Causa raiz.
    - Impacto.
    - Lições aprendidas.
    - Ações corretivas e preventivas.
- Compartilhar com todas as partes interessadas para alinhamento.

---

Revision #5
Created 2024-08-16 17:38:13 UTC by Wagner B. Simonato
Updated 2024-09-10 23:57:57 UTC by Wagner B. Simonato