Observabilidade, Detecção e Gestão de Eventos

O módulo de Observabilidade do Priax que permite a coleta de dados de Disponibilidade, Capacidade, Configurações, Logs e Eventos de Segurança a respeito dos Itens de Configuração, além de dados de performance de Aplicações, através de Tracing de suas transações. São armazenados dados históricos e gerados Alertas e Notificações para as equipes responsáveis por agir em cada situação distinta.

1. ## Monitoramento de Disponibilidade e Capacidade de Aplicações e Infraestrutura

   O Priax coleta dados em tempo real sobre o desempenho e a disponibilidade de Aplicações e suas transações e dos itens de configuração de TI presentes na CMDB, como servidores, bancos de dados, aplicativos, redes e dispositivos de armazenamento, bancos de dados, serviços, websites etc. Os dados são coletados continuamente com a finalidade de identificar problemas potenciais antes que eles afetem os serviços. Isso pode incluir a detecção de picos de uso, falta de capacidade, quedas de desempenho e falhas de hardware. São enviados alertas e notificações imediatas quando ocorrerem problemas ou quando determinados limiares forem atingidos. Isso permite que a equipe de TI responda prontamente e minimize o impacto nas operações.

   Para a visualização de dados históricos, o Priax possui uma interface visual intuitiva para exibir informações de desempenho e disponibilidade de forma clara e compreensível, sempre vinculado ao IC correlacionado. Além disso é possível gerar relatórios personalizados para acompanhar tendências, identificar gargalos e tomar decisões informadas sobre a capacidade do sistema além de realizar previsões de capacidade futura, ajudando a identificar possíveis gargalos ou necessidades de expansão antes que se tornem problemas reais. Além disso, o Priax é integrável com outros sistemas de gerenciamento e monitoramento, sistemas de gerenciamento de serviços (ITSM) e plataformas de automação, para permitir ações rápidas e automatizadas com base nos dados coletados.

2. ## Coleta e Análise de Logs

   Uma ferramenta de coleta e análise de logs de TI é fundamental para monitorar e

investigar eventos em hosts, sistemas, aplicativos e dispositivos de TI. O módulo de coleta e análise de Logs do Priax coleta logs de diferentes fontes, como servidores, roteadores, firewalls, sistemas operacionais e aplicativos, e envia para uma base de dados centralizada, vinculando cada log com o Item de Configuração correspondente facilitando o acesso, filtragem e a análise dos logs em um único local. Com os logs centralizados, são oferecidos mecanismos de filtragem e pesquisa avançada para localizar logs específicos com base em critérios como data, hora, origem, tipo de evento ou palavras-chave. Isso facilita a análise de eventos relevantes e a solução de problemas.
O Priax ainda é capaz de realizar análise estatística, identificar tendências, padrões ou anomalias nos logs ao longo do tempo além de correlacionar eventos de diferentes fontes para ajudar a identificar relações de causa e efeito entre diferentes registros. Isso é especialmente útil para investigar incidentes e entender melhor o contexto em que ocorreram e revelar insights valiosos sobre o desempenho, a segurança e a conformidade dos sistemas. Além disso, o Priax permite a configuração de alertas e notificações com base em determinados eventos ou padrões nos logs. Isso ajuda a detectar problemas em tempo real e a responder rapidamente a eventos críticos.

3. ## Detecção de Eventos de Segurança

Através da análise de logs com regras Sigma, o Priax pode identificar padrões que caracterizam ameaças conhecidas de segurança fornecendo uma visão em tempo real das atividades de segurança em uma rede, host ou sistema. Ele pode gerar alertas imediatos quando eventos suspeitos ou maliciosos são detectados. Atuando, portanto, como um SIEM, o Priax armazena logs e eventos de segurança em base de dados OpenSearch, permitindo a análise retrospectiva e a investigação de incidentes passados oferecendo recursos de pesquisa e análise avançados para identificar padrões e anomalias nos dados de segurança.
Os eventos são correlacionados, independente da fonte onde foi coletado para fornecer contexto e insights sobre as atividades de segurança, correlacionando cada evento de segurança detectado com o respectivo Item de Configuração ao qual ele se refere na CMDB sendo capaz de identificar relacionamentos entre eventos aparentemente não relacionados, ajudando a detectar ameaças avançadas e ataques complexos.

4. ## Mudanças em Configurações e Atributos dos ICs

A Auditoria de Configurações é a capacidade de uma ferramenta coletar, armazenar histórico e gerar alertas sobre alterações nos atributos e nas configurações dos ICs. O Priax realiza estas tarefas sobre os elementos cadastrados na CMDB, criando o controle necessário para implementar na práticas as políticas de mudanças e para facilitar o diagnóstico em casos de eventos causados por mudanças mal sucedidas. Com o armazenamento do histórico de cada mudança ocorrida em cada IC, podem ser realizadas análises retrospectiva, investigação e diagnóstico de eventos e incidentes, além de permitir a restauração de configurações anteriores para reestabelecer o funcionamento adequado de sistemas.

5. # Application Performance Monitoring (APM)

Além disso, o módulo de APM (Application Performance Monitoring) que permite o monitoramento de cada transação ocorrida internamente em cada aplicação e, alimenta o Discovery com dados que possibilitam o automático mapeamento das dependências das Aplicações monitoradas, correlacionando os Itens de Configuração consumidos cada aplicação.
O Priax possui um módulo de APM (Application Performance Monitoring) com capacidade de monitorar e gerenciar o desempenho de aplicativos em tempo real, coletando e analisando métricas relevantes, como tempo de resposta, taxa de erros, utilização de recursos (CPU, memória, disco), latência de rede e outros indicadores de desempenho. Além disso, realiza o monitoramento de transações e rastreamento de chamada de sistema, permitindo identificar gargalos e problemas de desempenho em chamadas de serviço, operações de banco de dados e outros componentes envolvidos nas transações. Todos esses dados alimentam também o Discovery com dados que possibilitam o automático mapeamento das dependências das Aplicações monitoradas, correlacionando os Itens de Configuração consumidos cada aplicação.
Todas essas funcionalidades oferecem recursos de detecção e diagnóstico de problemas de desempenho, ajudando a identificar a causa-raiz de problemas, como lentidão, erros ou falhas no aplicativo. Isso inclui a capacidade de rastrear a sequência de eventos e correlacionar dados de várias fontes para uma análise mais profunda e permitir a identificação de tendências e a capacidade para ajudar a prever e planejar o desempenho futuro do aplicativo. Isso inclui a identificação de padrões de uso, demanda de recursos e estimativas de crescimento para garantir uma infraestrutura escalável e adequada.

Para entregar tais resultados o APM se utiliza das seguintes funcionalidades:

a. Coleta e Análise de Logs, Traces e Métricas

O Priax APM realiza uma coleta e análise abrangente de logs, traces e métricas, realizando a observação Fim-a-Fim das Aplicações, registrando e avaliando os seguintes pontos:

- Requisição do usuário: Captura as ações do usuário no navegador, incluindo clicks e carga de páginas, gerando tráfego no servidor e registrando os tempos de atendimento de requisições ao navegador do usuário.
- Execução de métodos e trechos de códigos fontes: Monitora a execução do código nos servidores de aplicação.
- Consultas a bancos de dados: Analisa as consultas realizadas aos servidores de banco de dados.
- Identificação de comunicação HTTP(s): Detecta webservices e chamadas a serviços externos das transações de uma aplicação.
- Contexto de execução de métodos e transações: Correlaciona e contextualiza as transações das aplicações com os logs monitorados.

- Suporte a Diferentes Tipos de Métricas: A solução suporta métricas como tempo de resposta, latência e throughput, permitindo uma análise detalhada de métricas específicas (drill-down).
- Armazenamento e Análise de Histórico de Métricas: O histórico de métricas é armazenado para permitir análises retroativas, identificando padrões e tendências de desempenho.
- Análise Detalhada de Traces: A ferramenta permite um drill-down para análise detalhada de traces específicos, facilitando a investigação aprofundada de eventos.
- Rastreamento de Dados em Tempo Real: Os dados (traces) são rastreados em tempo real a partir de diferentes fontes, permitindo a identificação automática e inteligente do impacto do problema e sua causa raiz.
- Configuração Automática de Limites e Alertas: A ferramenta configura automaticamente os limites de cada indicador para os quais devem ser gerados alertas. Tal aprendizado é baseado em dados históricos do comportamento do ambiente e suas aplicações que são usados para ajustar automaticamente o comportamento da ferramenta. Este baseline de comportamento permite detectar desvios no comportamento das aplicações/transações, evitar falsos positivos e falsos negativos.
- Definição Inteligente de Critérios para Problemas e Incidentes: A solução define automaticamente e de forma inteligente os critérios para problemas e incidentes, considerando o histórico e o comportamento do ambiente.

Identificação de Problemas e Erros: A solução identifica problemas e erros no ambiente, analisando automaticamente os incidentes e os relacionamentos entre os componentes. Utiliza inteligência artificial para separar causa e efeito, apontando problemas agrupados em tempo real e mantendo um histórico dos problemas ocorridos.

b. Coleta e Análise de Comportamento do Usuário

A solução de observabilidade oferece funcionalidades avançadas para a coleta e análise do comportamento dos usuários das aplicações, atendendo a diversos requisitos específicos tais como:

- Identificação do Perfil dos Usuários: A solução coleta e identifica o perfil dos usuários das aplicações, considerando dados como localização física do usuário, tipo de dispositivo navegador, sistema operacional, tempo de acesso, quantidade de requisições, tempo médio de permanência, registro de cliques e uso de serviços.
- Identificação de Usuários que regressam à aplicação.
- Correlação de Dados de Comportamento: Os dados de comportamento dos usuários são correlacionados com métricas de negócio e de desempenho, proporcionando uma visão integrada do impacto do comportamento do usuário nas operações.
- Integração com Ferramentas de Análise de Experiência: A solução permite a integração com ferramentas de análise de experiência do usuário, como mapas de calor, para uma análise visual detalhada.
- Análise das Atividades de Acesso: A solução coleta e analisa a forma de acesso às aplicações, identificando atividades de entrada e atividades de saída, registrando o volume e o tempo médio de duração dessas atividades.

- Verificação da Performance das Ações dos Usuários: A ferramenta verifica a performance das ações dos usuários, exibindo na linha do tempo a quantidade de ações, a duração, a situação e o tempo de execução das ações.
- Informações sobre Ações dos Usuários: Disponibiliza informações detalhadas sobre as principais ações dos usuários nas aplicações, indicando o total de ações executadas por período e exibindo informações sobre o tempo de contribuição das ações, incluindo o tempo total da experiência, tempo de execução do servidor, tempo de renderização do HTML, tempo de DNS e tempo de conexão com o servidor.
- Informações sobre Erros de JavaScript: Para erros de JavaScript identificados nas aplicações, a solução apresenta informações detalhadas como sistema operacional de origem, navegador, localidade e ação que gerou o erro, indicando a quantidade de erros ocorrida por categoria.
- Compatibilidade com com métricas de experiência de usuários baseados no Google Core Web Vitals.

c. Monitoramento e Análise de Desempenho da Aplicação

A solução oferece funcionalidades abrangentes para monitoramento e análise de desempenho das aplicações hospedadas em um Data Center incluindo:

- Monitoramento de Performance de Servidores de Aplicação (APM): Monitora a performance de servidores de aplicação conforme as características e tecnologias especificadas.
- Identificação de Problemas e Causa Raiz: A solução identifica problemas ou incidentes nas aplicações, apontando automaticamente a causa raiz e indicando a camada onde o problema ocorreu (ex.: aplicação, serviço, webservice, servidor, web, rede, usuário).
- Suporte à ampla lista de tecnologias: Monitora aplicações construídas com a maioria de pilhas tecnológicas de back-end e front-end.
- Comparação de Desempenho: Permite a comparação do desempenho das aplicações pela perspectiva do usuário.
- Informações sobre Aplicações: Proporciona informações sobre número de sessões, requisições HTTP, tempo de atendimento, volume de falhas dos serviços e dependências do serviço.
- Tempo de Carregamento de Página: Coleta e analisa o tempo exato de carregamento da página até que esteja completamente pronta para uso, separando a métrica por localidade, tipo de dispositivo, localização, sistema operacional ou tipo de navegador.
- Análise de performance de aplicações adjacentes: Verifica automaticamente a performance e disponibilidade dos principais serviços acessados pela aplicação instrumentada, mesmo que tais aplicações adjacentes não estejam instrumentadas, extraindo dados a respeito de médias de latência, transferência de dados e taxa de transações com falhas.
- Descoberta Automática de Processos e Dependências: Descobre automaticamente todos os processos, serviços, aplicações e suas respectivas dependências entre hosts e processos.
- Topologia Dinâmica da Aplicação: Descobre automaticamente a topologia da aplicação, apresentando um mapa completo e atualizado das dependências entre componentes sem intervenção manual.

- Visualização da Performance do Ambiente: Acompanha a performance do ambiente de forma visual, verificando latência, transferência de dados e taxa de erros por serviço, identificando o código-fonte dos erros.
- Análise Detalhada de Serviços e Métodos: Verifica a performance dos serviços e métodos, monitorando tempos de resposta, utilização de CPU, requisições por período, taxas e quantidade de falhas.
- Identificação de Dependências de Serviços: Identifica as aplicações que usam serviços específicos e os bancos de dados e comandos SQL acessados.
- Fluxo Gráfico das Requisições: Apresenta um fluxo gráfico das requisições que chamam e que são chamadas por um serviço em análise.
- Verificação de Performance de Garbage Collection: Monitora a execução e a performance dos processos de Garbage Collection.
- Distribuição dos Tempos de Resposta: Produz gráficos de tempos de resposta detalhando a distribuição por fases da transação e pelo métodos do código fonte para identificar a distribuição do tempo total utilizado para atendimento de cada requisição.
- Visão Gráfica do Ambiente: Apresenta uma visão gráfica da aplicação monitorada, contendo mapas, painéis e gráficos personalizados das principais métricas e análises, permitindo filtros por períodos históricos.
- Mapeamento Automático de Componentes: Mapeia automaticamente os componentes e seus relacionamentos que sustentam as aplicações, incluindo serviços, processos e infraestrutura.
- Métricas de Ações indexados por Usuários: Apresenta métricas como volume de dados baixados, tempo médio de interatividade do usuário, tempo no servidor, tempo no navegador e tempo de tráfego de rede.
- Monitoramento de Recursos de Infraestrutura: Correlaciona dados de infraestrutura com os dados da aplicação monitorada na mesma escala de tempo.
- Monitoramento de execuções SQL: Monitora a execução das instruções SQL, apresentando quantidade de execuções, taxa de falhas e tempo médio de resposta criando gráficos da distribuição dos tempos de resposta das consultas a banco de dados.
- Rastreamento de Aplicações e Serviços: Permite rastreamento das aplicações e serviços que executaram comandos de banco de dados.
- Correlacionamento de Problemas com Deploy: Disponibiliza informações sobre eventos como restart ou deploy, correlacionando problemas com possíveis problemas no processo de deploy.
- Identificação e Análise de Falhas: Oferece funcionalidades para identificar e analisar falhas das aplicações, avaliando automaticamente os níveis de qualidade, gerando alertas, reduzindo a quantidade de eventos em ambientes críticos, e correlacionando subeventos.
- Detalhamento de Tempos de Execução: Apresenta detalhamento de tempos de execução em nível de classe, método e comandos SQL para transações com desvios de comportamento.
- Identificação Automática de Problemas: Identifica automaticamente transações, queries SQL e serviços de backend com baixa performance ou indisponíveis.
- Detalhamento de Métodos Executados: Exibe os métodos executados nas transações com problemas de performance sem necessidade de configuração manual.

- Impacto dos Problemas: Aponta o número de aplicações e componentes de infraestrutura afetados pelos problemas identificados.

d. Monitoramento e Análise dos Acessos e Segurança de Aplicações

A solução proporciona funcionalidades detalhadas para monitoramento e análise dos acessos e da segurança de aplicações tais como:

- Identificação de Usuários Autenticados: Identifica o usuário que está acessando a aplicação, identificando a região de origem, qualidade do acesso, tipo de navegador, versão do sistema operacional, IP de origem e comportamento temporal das ações.
- Registro de estatísticas: Registra o número simultâneo de usuários e o tempo médio de permanência dos usuários às aplicações.
- Detecção Automática de Transações Críticas: Detecta automaticamente transações críticas para o negócio que apresentam problemas ou desempenho abaixo do esperado.
- Controle de Acesso e Permissões: Possui controle de acesso e permissões, permitindo criar e modificar grupos de perfis de acesso.
- Armazenamento e Indexação de Dados de Acesso: Armazena e indexa os dados de acesso de forma eficiente e escalável.
- Correlacionamento de Dados de Acesso: Correlaciona dados de acesso com métricas de infraestrutura, logs de erros e eventos para identificar possíveis causas raiz.
- Identificação de Vulnerabilidades em Tempo Real: Identifica vulnerabilidades em tempo real, sem a necessidade de um scanner periódico.
- Integração com Ferramentas de Segurança: Integra-se nativamente ou via APIs com ferramentas de análise de segurança, scanners de vulnerabilidades e ferramentas de análise estática de código.
- Regras personalizáveis de segurança: Define regras e política de análise de segurança personalizadas atendendo necessidades específicas das aplicações.
- Monitoramento em Tempo Real: Monitora a aplicação em tempo real para detectar possíveis violações de segurança ou atividades suspeitas.
- Integração com Provedores de Inteligência de Ameaças: Integra-se com provedores de inteligência de ameaças para receber informações atualizadas sobre ameaças conhecidas e novas.
- Exportação de Dados de Segurança: Permite a exportação de dados de segurança para outras ferramentas de análise ou armazenamento.
- Análise de criticidade de Risco de Vulnerabilidades: Gera automaticamente uma classificação de risco para cada vulnerabilidade.
- Detalhamento de Problemas de Segurança: Exibe o número de problemas de segurança abertos, as aplicações monitoradas com vulnerabilidades encontradas e as tentativas de acesso nessas vulnerabilidades.
- Listagem de Vulnerabilidades: Lista todas as vulnerabilidades detectadas no ambiente monitorado, pontuando-as de acordo com o nível de risco.
- Detecção e Alertas de Segurança: Permite o envio de alertas de segurança às equipes para fins de alerta e correção.

- Integração com Ferramentas de Segurança: Integra-se com firewalls de aplicação, soluções de detecção de intrusão e sistemas de gerenciamento de informações e eventos de segurança (SIEM).

e. Coleta e Análise de Transações de Negócios

O Priax oferece funcionalidades avançadas para coleta e análise de transações com interpretação de lógicas de negócio possibilitando uma análise com uma visão interpretativa que ofereça insights valiosos.
Neste sentindo o Priax oferece:

- Análise em Tempo Real: A solução possibilita a análise de transações de negócio em tempo real para identificar ações relevantes de usuários executadas nas aplicações. Isso inclui evolução em etapas de processos, conversões, assinaturas, vendas, matrículas e qualquer outra ação que faça sentido para o negócio, podendo ser essas ações customizáveis.
- Correlação de Métricas: É possível realizar correlação de indicadores do negócio com métricas de desempenho de transações e infraestrutura proporcionando uma visão unificada do desempenho de negócios e de sistemas.
- Exportação de Dados: A solução permite a exportação de dados de transações de negócio para análise em outras ferramentas, facilitando a integração com sistemas de análise externa.
- Detecção Automática de Transações: A detecção de transações de negócio ocorre automaticamente ou via Opentelemetry, baseando-se em protocolos e tecnologias como HTTP/HTTPS, webservices, serviços de mensageria (Kafka, MQ), chamadas externas à sistemas externos, spring, entre outros métodos.
- Visão Gráfica da Topologia: Podem ser criados dashboards que representam a topologia de um processo de negócio, oferecendo uma representação visual do fluxo de negócios e da dependência, precedência e sucessão entre componentes.
- Monitoramento de Execuções: O monitoramento das execuções das transações de negócio inclui métricas mínimas como quantidade de execuções, tempos de resposta e volume de erros. Oferece um drilldown detalhado do código executado (classes e métodos) para transações que se desviam do padrão normal de funcionamento.
- Classificação e Quantificação de Execuções: A solução classifica e quantifica a execução das transações de acordo com o tempo de resposta e eventuais erros, fornecendo essa análise em nível de aplicação, transação de negócio e servidor de aplicação.

Revision #3
Created 2024-06-07 17:12:54 UTC by Wagner B. Simonato
Updated 2024-09-10 17:35:53 UTC by Wagner B. Simonato