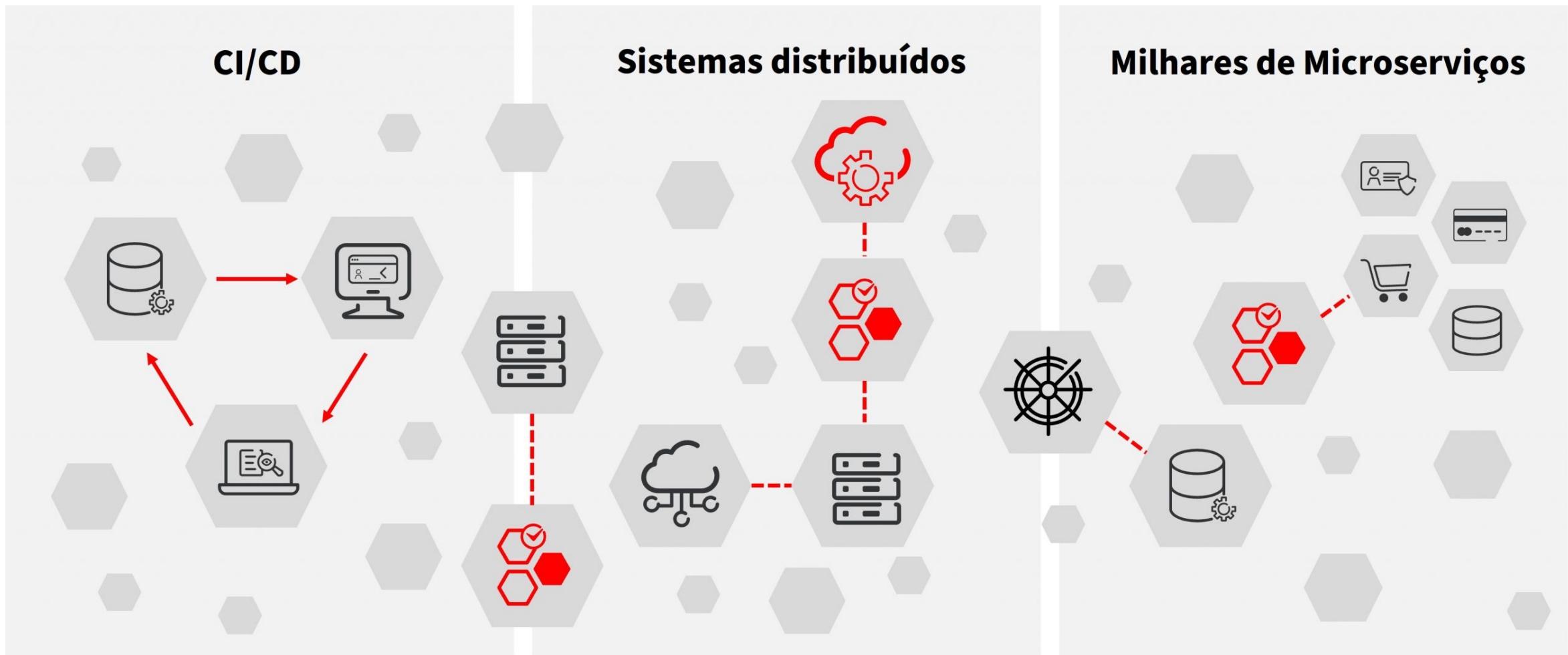


Monitoramento e observabilidade

Paulo Henrique Nazaré

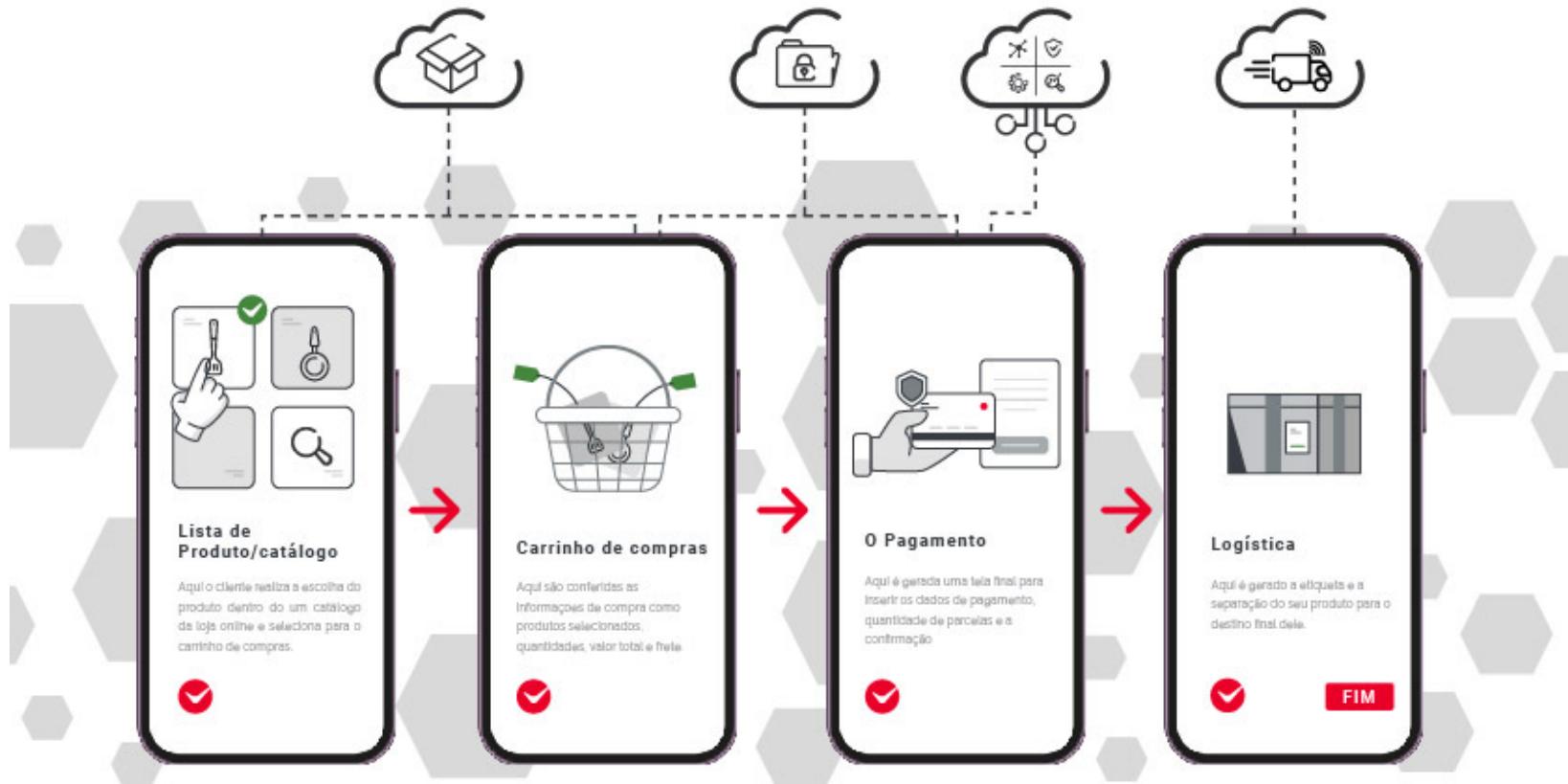
Estratégias para medições e monitoramento contínuo.

Observabilidade



Fonte da imagem : redhat.com

Comércio eletrônico



Fonte da imagem : redhat.com

Observabilidade

A expectativa dos **consumidores aumentou e a tolerância para erros diminuiu**. **Plataformas Digitais lentas, propensas a erros ou mal projetadas são um grande obstáculo**. Hoje, as organizações têm a possibilidade de trabalhar com arquiteturas de microserviços e sistemas distribuídos em várias soluções Cloud Native. Elas são mais fáceis de adotar e funcionam juntas de maneira cada vez mais integrada. As empresas estão se organizando em torno de equipes autônomas responsáveis

Observabilidade

A Observabilidade Inteligente reúne todos os dados e traz a I.A. para o core para analisar automaticamente as dependências entre os componentes de um sistema, identificando não apenas se um serviço problemático é a causa raiz de um problema, mas também suas dependências de outros serviços que são executados em diferentes grupos de processos no seu datacenter ou nuvem. Como resultado, com um clique, você agora pode mergulhar fundo nas **Métricas, Rastreamentos e Eventos** envolvidos para entender e corrigir o problema.

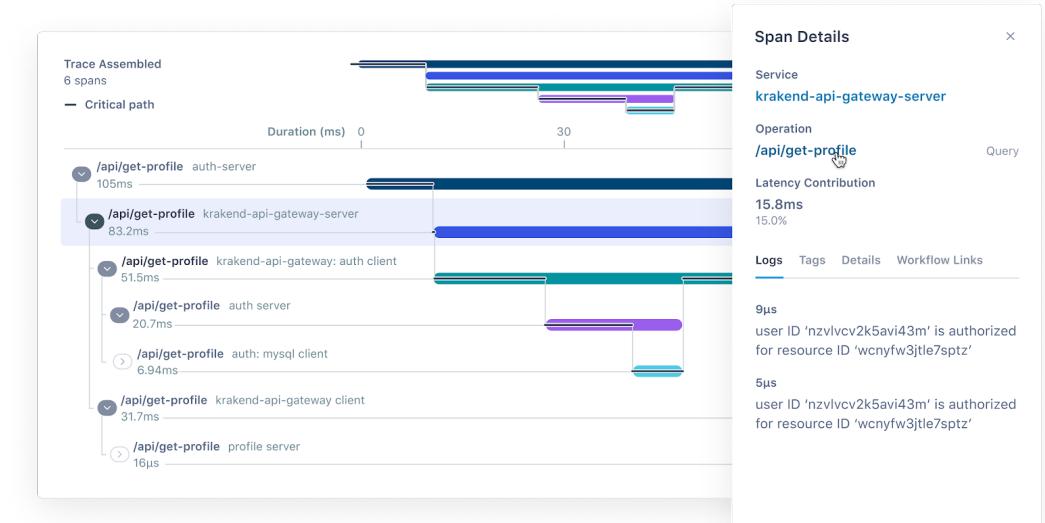
Observabilidade

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET  
/apache_pb.gif HTTP/1.0" 200 2326
```

Logs



Métricas



Traces - Rastreamentos

Observabilidade

Os ambientes estão em mudança constante, da relação de dependência dos sistemas com a infraestrutura até o fluxo dos serviços que os compõem, a Observabilidade Inteligente te ajuda a estar sempre atualizado sobre estas mudanças, porque conta com o mecanismo de mapeamento contínuo e automatizado dos dados que mostra em tempo real os relacionamentos e as dependências de todas as entidades, tanto verticalmente na pilha, como horizontalmente entre serviços e suas transações.

Observabilidade – Como pode ajudar

- MAIS FÁCIL – redução drástica de todas as atividades manuais de implementação, configuração e análise de monitoração. Uma forma pronta para uso onde o ambiente seja continuamente descoberto e mapeado, com todas as dependências, da infraestrutura ao código, do click de cliente a chamada ao banco de dados, com todos os dados reunidos e relacionados (métricas, traces, logs, e KPIs de Negócio).



FONTE : LINKEDIN

Observabilidade – Como pode ajudar

COM RESPOSTAS – para acelerar o entendimento do ambiente, comportamento e problemas.

- Retirar o ruído de falsos positivos e tempestades de alertas;
- Onde alertas venham explicando onde está o problema, qual serviço e clientes impactados;
- Permitindo a automação de remediação e da comunicação unificada com todos os times, para que possam atuar unidos na solução do problema, no apoio ao negócio e no atendimento ao cliente.



Observabilidade – Como pode ajudar

GERE VALOR – sendo relevante no dia a dia das equipes de Dev, Ops e Suporte (impacto na capacidade produtiva e na eficiência operacional e de decisão).

- Recuperando a capacidade operacional das equipes, liberando as pessoas das atividades manuais relacionadas a monitoração, instrumentação e análise de problemas (Dev/QA e Ops);



FONTE : LINKEDIN

Observabilidade – Como pode ajudar

- Aumentando a eficiência operacional engajando corretamente as pessoas onde elas de fato precisam ser envolvidas;
- Aumentando a produtividade das equipes, agora que elas estão focadas na inovação e no negócio, e não usando a maior parte do tempo cuidando de ferramentas de monitoração e procurando a agulha no palheiro.



FONTE : LINKEDIN

Observabilidade – Benefícios diretos

O uso das tecnologias corretas e realizadas com base nas boas práticas da abordagem é possível acelerar e inovar de forma mais rápida, inteligente e fácil onde:

-  Ops Operando com mais eficiência com:
 - 40% Redução de Tickets e Incidentes;
 - 95% Redução de Esforço em Administração da Monitoração;
-  Dev/QA Inovando mais rápido com confiança e maior qualidade com:
 - 45% Menos Esforço em Análises, Labs e Correções;
 - 95% Redução de Esforço para Observabilidade;
-  – Maior Produtividade dos Usuários;
 - Redução de Chamados no Service desk;

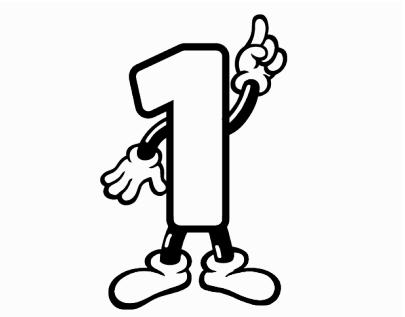


PUC Minas Virtual

Os três principais elementos da observabilidade.

Open instrumentation (Instrumentação aberta)

É definido como a coleta de código aberto ou dados de telemetria específicos do fornecedor de um aplicativo, serviço, host de infraestrutura, contêiner, cloud native, função sem servidor, aplicativo móvel ou qualquer outro tipo de emissão de dados. Com open instrumentation há o fornecimento de visibilidade para toda a superfície de aplicações e infraestrutura que são essenciais aos negócios



Entidades conectadas

Todos os dados de telemetria devem ser analisados para que as entidades que os produzem possam ser identificadas e conectadas, os metadados também precisam ser incorporados para criar correlação entre estas entidades e seus dados. Estas duas ações criam contexto e significado a partir de grandes volumes de dados. A partir daí, a curadoria pode ser entregue em forma de modelos visuais do sistema sem qualquer configuração adicional. Além disso, a inteligência pode ser aplicada para agregar ainda mais significado. Inteligência aplicada é a aplicação de aprendizado em ciência de dados com finalidade de procurar padrões ou anomalias para que as equipes possam tomar decisões e agir corretamente.



Contextualização

Cada empresa é única e nenhuma curadoria automática pode atender a todas as suas diferentes necessidades. As organizações precisam criar seu próprio contexto sobre seus dados de telemetria, combinando dados críticos e dimensões de negócios. É importante ter a capacidade de mostrar claramente o custo dos erros e falhas em um processo de negócio e fornecer um caminho para analisar os dados para, então, encontrar o verdadeiro motivo.





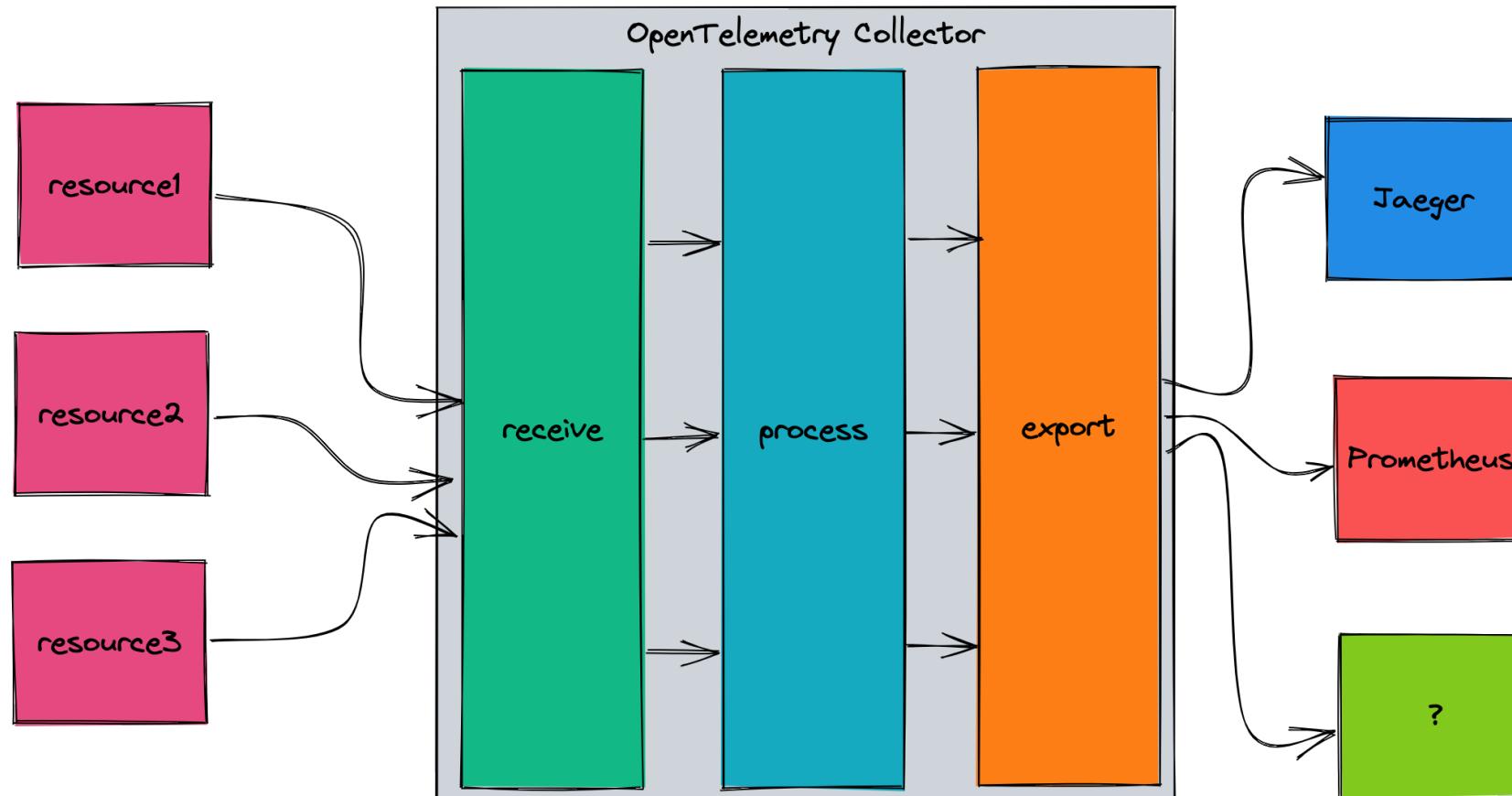
PUC Minas Virtual

OpenTelemetry.

OpenTelemetry

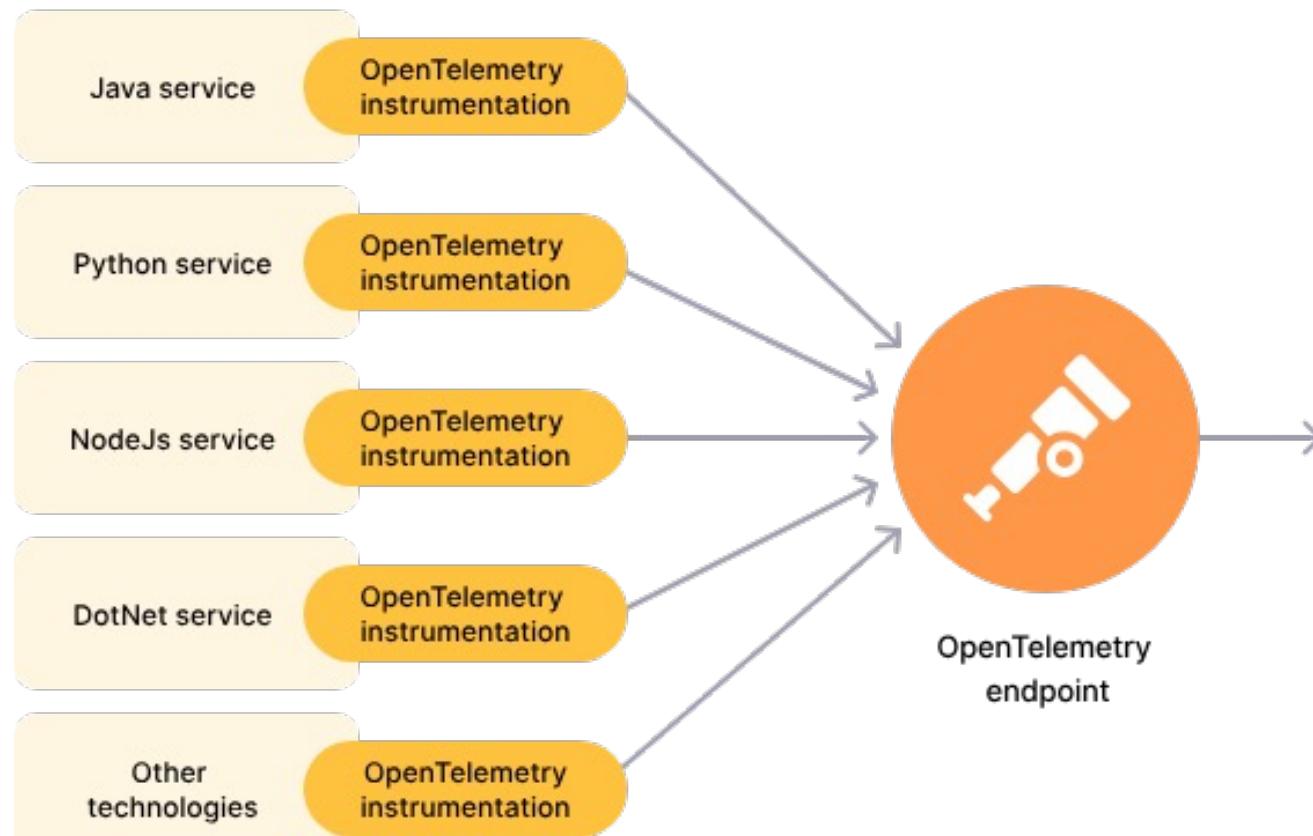
Com a crescente necessidade de usar diferentes aplicações para executar processos, fornecer serviços e colher dados, a observabilidade em sistemas ficou mais complexa. O OpenTelemetry vem justamente atuar no cerne do problema, ao permitir centralizar os processos de observabilidade de diferentes aplicações. Com a evolução da computação distribuída, tem sido exigida dos desenvolvedores e dos responsáveis pela gestão dos sistemas uma maior atenção à observabilidade. A complexidade cada vez maior dos microsserviços e das aplicações torna mais difícil identificar os logs das aplicações, suas saídas, e quando querys e serviços estão com tempo de resposta mais elevado do que o normal.

OpenTelemetry

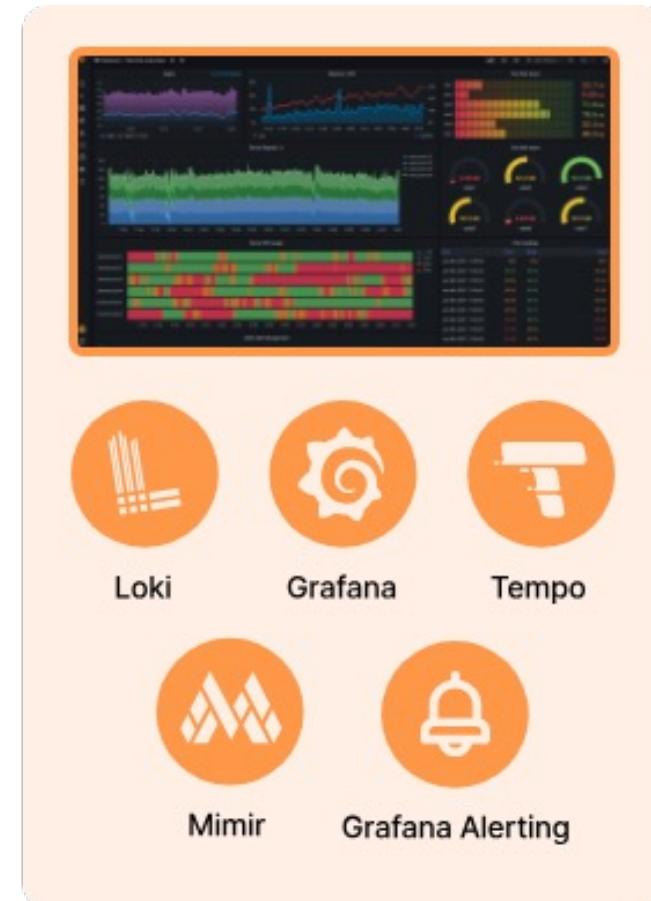


Fonte da imagem : [Grafana.com](https://grafana.com)

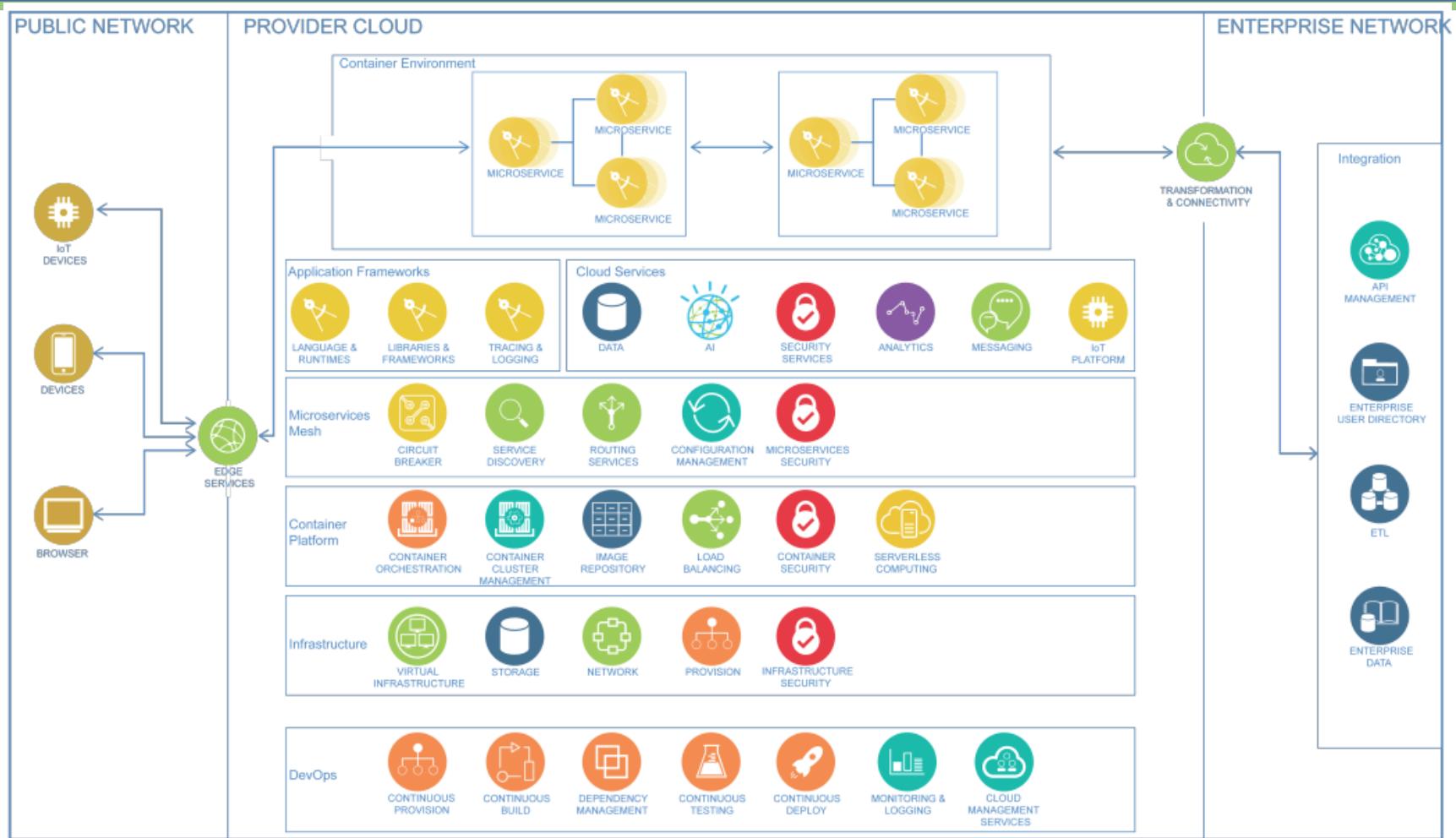
OpenTelemetry



Fonte da imagem : [Grafana.com](https://grafana.com)



OpenTelemetry

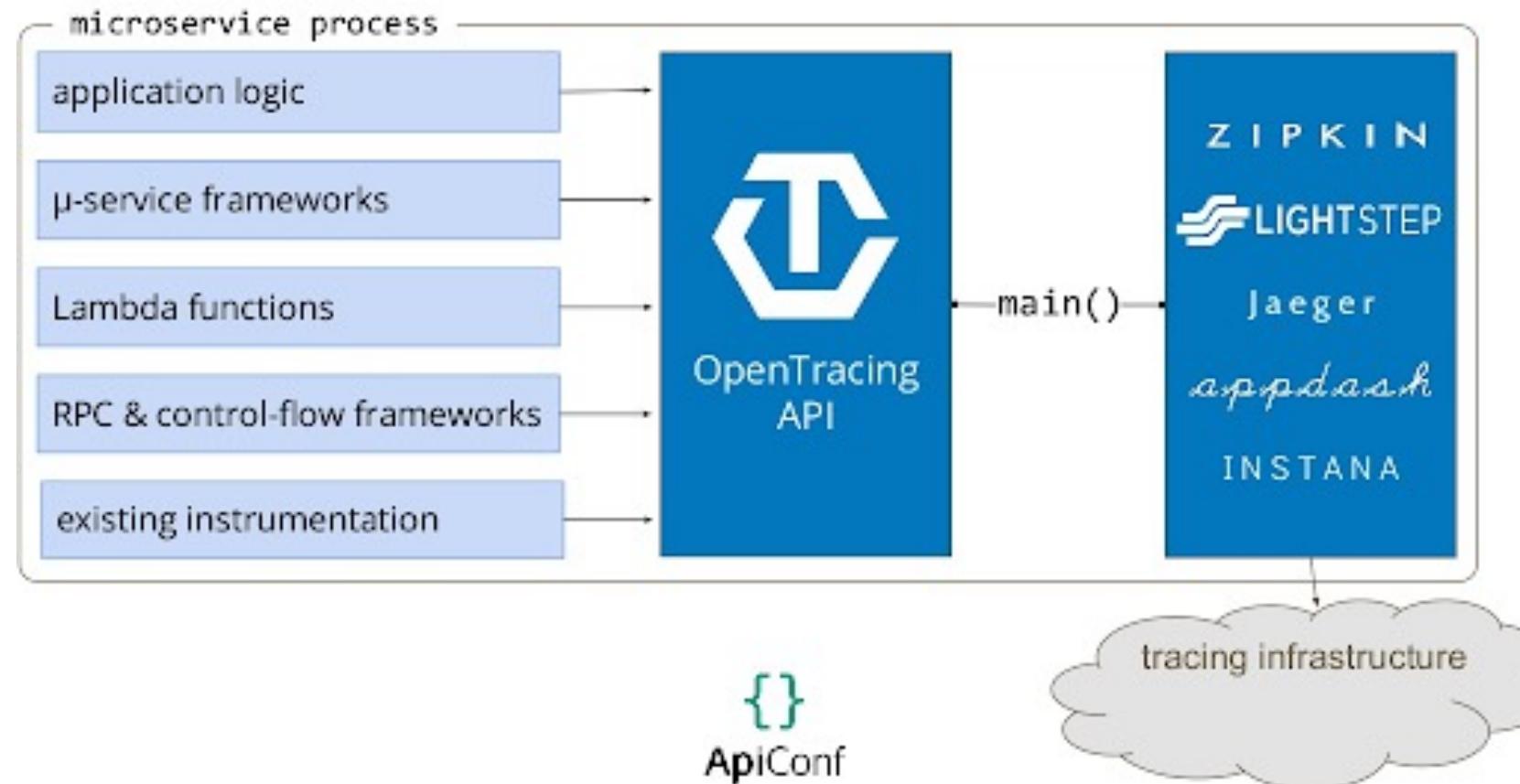


Fonte da imagem : [Grafana.com](https://grafana.com)

OpenTelemetry

A criação do OpenTelemetry foi a solução encontrada pelos profissionais de **DevOps** e gestores para tornar a observabilidade das aplicações **agnóstica aos vendors**, ou seja, centralizar as ações para “driblar” as voltas que normalmente são dadas para elevar a capacidade de monitoramento. OpenTelemetry combinou os projetos **OpenTracing** e **OpenCensus** para aprimorar a observabilidade de sistemas e aplicações em rede.

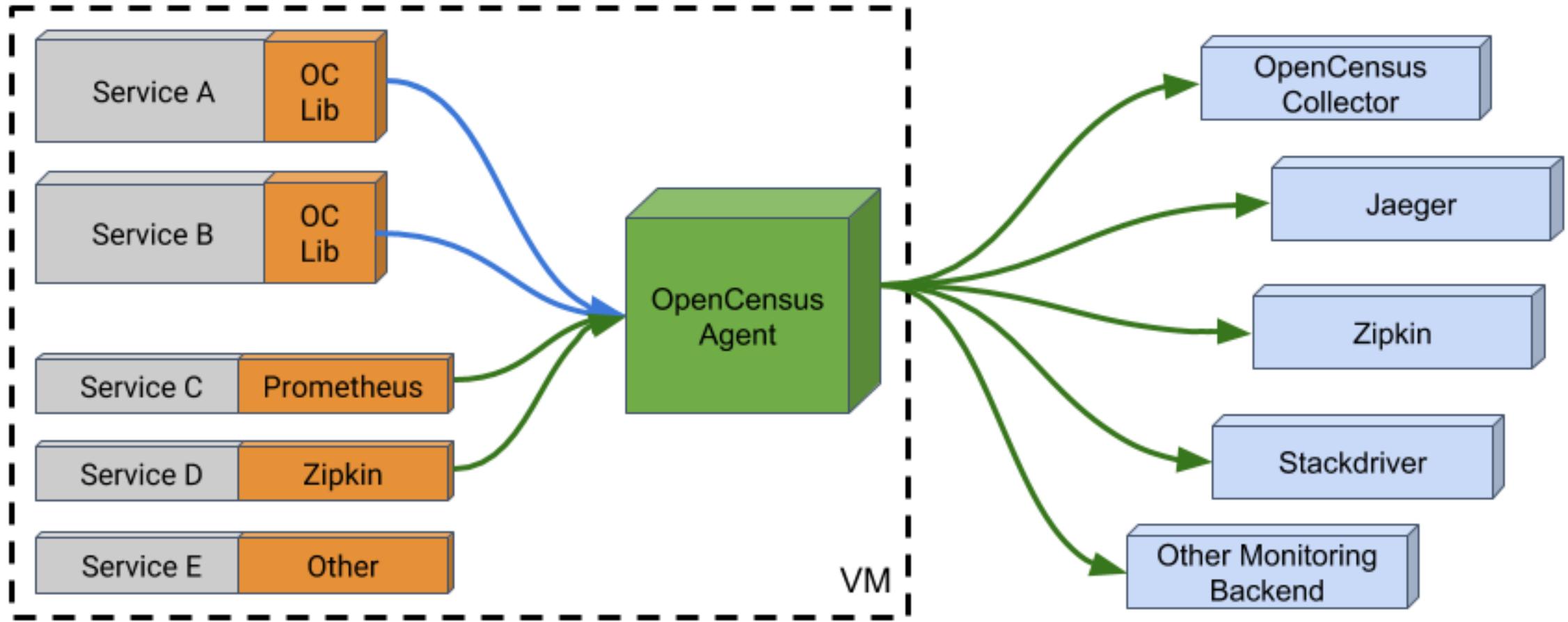
OpenTelemetry



OpenTelemetry - OpenCensus

O OpenTracing foi uma iniciativa de padrão aberto, voltada para a criação de uma aplicação que conseguisse direcionar o desenvolvimento de frameworks e rastrear rapidamente o caminho feito **por logs**, aberturas de chamadas, etc. Ou seja, seu foco é o tracing distribuído.

OpenTelemetry - OpenCensus



OpenTelemetry

O OpenTelemetry é justamente a combinação das funções do OpenTracing e do OpenCensus em uma só aplicação, elevando a capacidade de observabilidade dos microserviços. Por isso, vem sendo considerado o futuro da telemetria instrumental.

Ainda como aplicação de código aberto, o OpenTelemetry foca em três pilares:

- Rastreamento distribuído
- Métricas
- Logs

OpenTelemetry

Entre as funções mais importantes do OpenTelemetry, estão:

- Monitoramento de integridade dos microsserviços.
- Atribuição do uso de recursos a grupos de usuários segmentados.
- Criação de solicitações prioritárias entre recursos compartilhados.

OpenTelemetry – como funciona ?

- OpenTelemetry permite customizar as ferramentas para trabalhar em diferentes contextos de DevOps, de acordo com as necessidades da equipe.
- O Collector é a função que permite gerar, coletar, processar e exportar para o vendor os dados de telemetria de forma padronizada, logo, ele é o componente principal para execução dos objetivos. Porém, com o OpenTelemetry, **o Collector não mais dependerá do vendor fornecedor**, sendo, portanto, o que chamamos anteriormente de uma aplicação agnóstica.



PUC Minas
Virtual

Conexão do monitoramento e observabilidade com as estratégias de SLO e Error Budgeting

Perguntas de Observabilidade pode responder

- De quais serviços o meu serviço depende — de quais serviços dependem meu serviço?
- O que deu errado durante o deployment?
- Por que o desempenho se degradou em um determinado período ?
- O que mudou? Por que?
- Quais registros devemos olhar agora?
- Devemos reverter este cenário?
- Qual SLO devemos definir?
- O que provavelmente está contribuindo para a latência agora?
- Essas otimizações de desempenho estão no caminho crítico?

Perguntas de Observabilidade pode responder



SLOs:
Service level objectives

O que são os SLOs?

Os SLOs fazem parte de um conjunto de medidas que visam aumentar a qualidade do gerenciamento do serviço. Entre elas podemos citar os service level indicators (SLIs), os service level objectives (SLOs) e os service level agreements ([SLAs](#)). Esse conjunto de medidas ajuda a entender quais comportamentos realmente importam, como medi-los e de que forma avaliá-los para que o serviço tenha um nível de qualidade aceitável. Escolher as métricas apropriadas garante que as ações corretas sejam realizadas caso algo dê errado. Isso traz maior confiança para o time de Site Reliability Engineering (SRE) sobre o que é importante para o pleno funcionamento do serviço, além de resultar em uma experiência positiva ao usuário final.

Terminologias

É importante você entender algumas terminologias :

- **Service Level Indicators (SLIs)**: São as métricas utilizadas para medição do nível de serviço fornecidos aos usuários finais, como disponibilidade, latência, taxa de transferência, etc.
- **Service Level Objectives (SLOs)**: São os níveis de serviço que se visa atingir, que são medidos pelos SLIs. Normalmente são expressos em percentuais ao longo de um período de tempo.
- **Service Level Agreements (SLAs)**: São os acordos contratuais que tratam do nível de serviço esperado pelos usuários finais. Caso esses acordos não sejam cumpridos, podem haver consequências.
- **Error budgets**: São os níveis aceitáveis de falta de confiabilidade para um serviço antes que ele se enquadre como fora da conformidade no SLO.

Como criar um Service level objectives (SLO)

Para criar os SLOs você deve levar em consideração o que ele deve cobrir. Sua principal missão é garantir um alto nível de confiabilidade para os usuários finais. Para isso, é preciso saber como o seu usuário utiliza seu sistema e quais as jornadas dos usuários são as mais críticas. A seguir elencamos algumas perguntas que podem te ajudar na hora de definir seus objetivos quanto ao nível de serviço:

- Como os usuários fazem uso de suas aplicações?
- Qual jornada eles percorrem no aplicativo?
- Quais são as partes da infraestrutura que a jornada depende?
- O que é esperado das aplicações e o que os usuários esperam realizar nela?

Exemplos de Service level objectives (SLO)

API

Na conexão com API o dado analisado foi a disponibilidade da infraestrutura.

Categoria	SLI	SLO
Disponibilidade	quantidade de vezes em que a API foi consultada e retornou os dados com sucesso.	97% das vezes de conexão sendo bem sucedidas.

Exemplos de Service level objectives (SLO)

API

Na conexão com API o dado analisado foi a disponibilidade da infraestrutura.

Categoria	SLI	SLO
Disponibilidade	quantidade de vezes em que a API foi consultada e retornou os dados com sucesso.	97% das vezes de conexão sendo bem sucedidas.

Exemplos de Service level objectives (SLO)

HTTP

Com a categoria de servidor público (HTTP) o dado analisado é a latência, que é o tempo entre um comando ser executado até a sua resposta.

Categoria	SLI	SLO
Latência	A velocidade de resposta do servidor.	90% das respostas do servidor serem < 200 ms e 99% das respostas serem < 1,000 ms

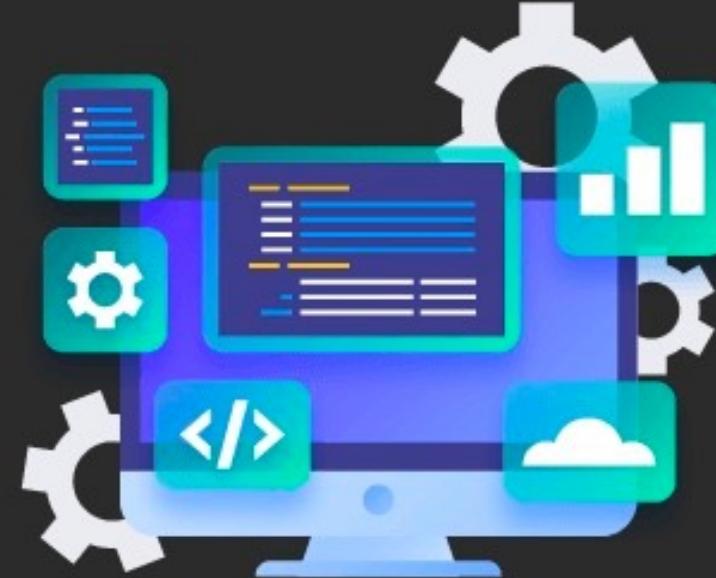


PUC Minas Virtual

Principais ferramentas de monitoramento.

Ferramentas de monitoramento

Stacks para
OBSERVABILIDADE



Ferramentas de monitoramento

As ferramentas de observabilidade desempenham um papel fundamental no monitoramento e na análise de sistemas complexos, trazendo às equipes DevOps uma visão abrangente do comportamento dos aplicativos e da infraestrutura.

Ferramentas de monitoramento

1 – Prometheus

O Prometheus é uma ferramenta de código aberto amplamente adotada para monitorar e alertar sobre a saúde de sistemas e aplicações. Seu destaque fica para a arquitetura simples e flexível, que permite a coleta e o armazenamento eficiente de métricas. Com suporte para consultas e alertas, ele oferece uma visão detalhada do comportamento do sistema e ajuda a identificar gargalos e problemas de desempenho.

Ferramentas de monitoramento

Prometheus



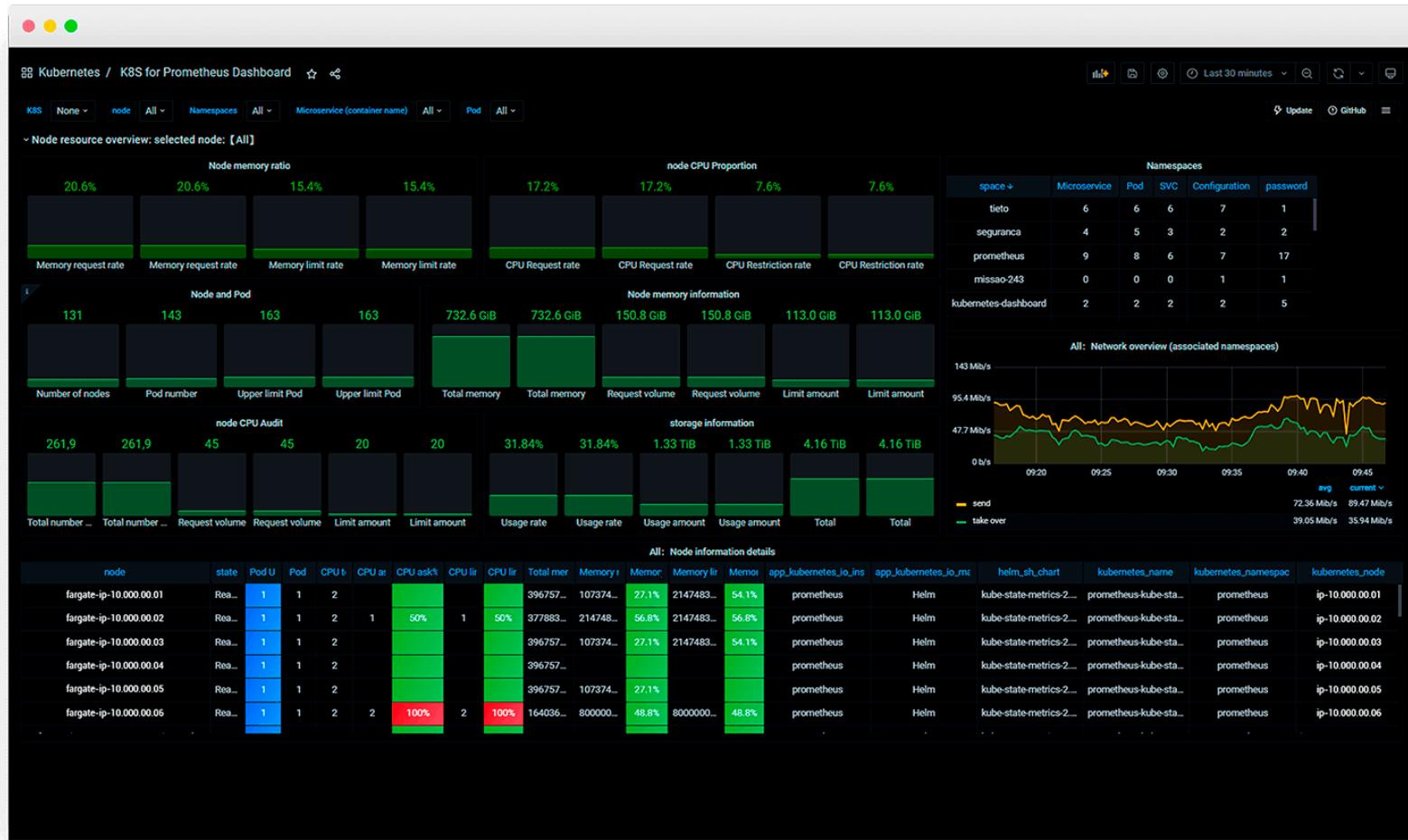
Ferramentas de monitoramento

2 – Grafana

Essa plataforma de visualização de dados é amplamente utilizada e consegue se integrar facilmente ao Prometheus, entre muitas outras ferramentas. O Grafana conta com uma interface intuitiva, permite criar painéis personalizados e gráficos interativos para monitorar métricas e logs em tempo real. Além disso, oferece recursos de alerta, o que permite que as equipes configurem notificações com base em condições específicas.

Ferramentas de monitoramento

Grafana



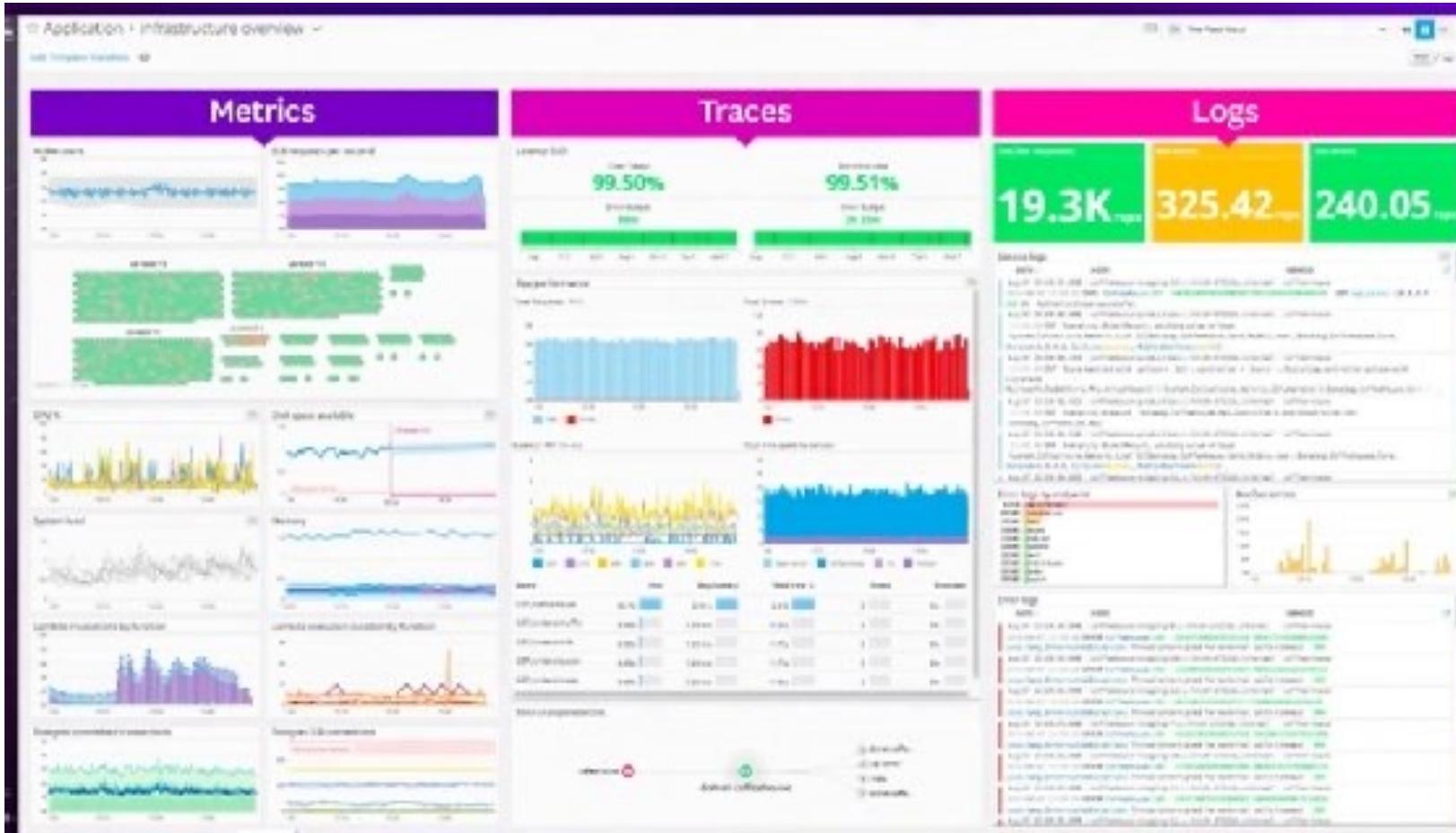
Ferramentas de monitoramento

3 – DataDog

Permite o monitoramento de métricas, logs e traces de aplicações. Também conta com recursos de alerta, análise de tendências e integração com outras ferramentas populares.

Ferramentas de monitoramento

Data Dog



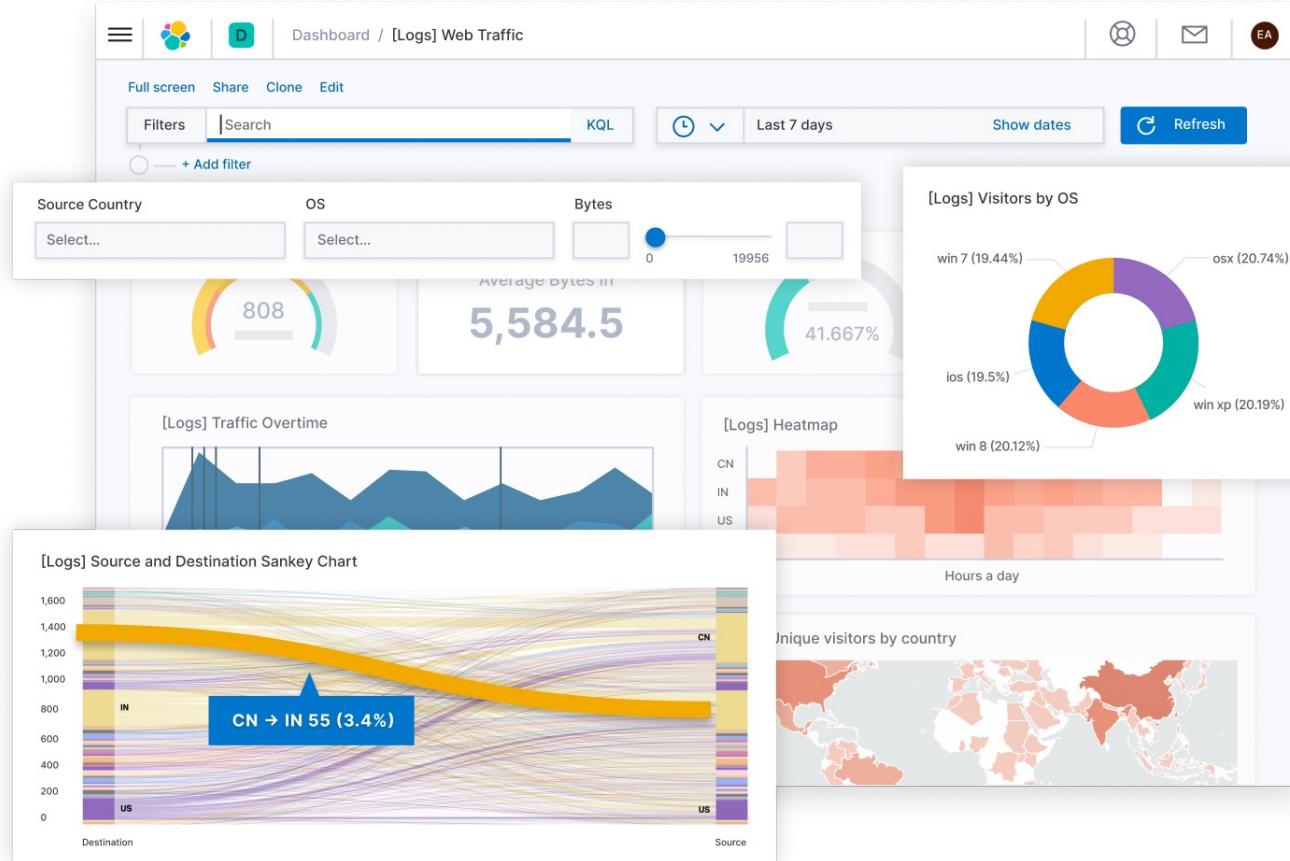
Ferramentas de monitoramento

4 - ELK Stack (Elastic Stack)

O ELK Stack é uma suíte de ferramentas poderosa para observabilidade de logs e análise de eventos composto pelo Elasticsearch, Logstash e Kibana. Permite a indexação e pesquisa eficiente de grandes volumes de logs, enquanto o Logstash facilita a coleta, transformação e envio de logs para o Elasticsearch. Já o Kibana oferece uma interface intuitiva para visualizar, pesquisar e criar painéis com base nos dados de log coletados, ajudando a identificar padrões, anomalias e tendências.

Ferramentas de monitoramento

ELK Stack (Elastic Stack)



Ferramentas de monitoramento

5 – Dynatrace

Ferramenta que combina monitoramento de desempenho, rastreamento de transações e inteligência artificial para fornecer insights acionáveis sobre o ambiente de TI. Conta com recursos avançados de detecção automática de dependências e análise de causa raiz, também ajuda as equipes a entenderem o impacto das alterações de código e a identificarem gargalos de desempenho em tempo real.

Ferramentas de monitoramento

Dynatrace





PUC Minas
Virtual

Abordagem de instrumentação e monitoramento SRE

Engenharia de confiabilidade de sites (SRE) é uma abordagem da engenharia de software às operações de TI. As equipes de SRE usam software como uma ferramenta para gerenciar sistemas, solucionar problemas e automatizar tarefas operacionais. Na abordagem de SRE, as tarefas que historicamente eram realizadas pelas **equipes de operações**, muitas vezes manualmente, passam a ser delegadas a engenheiros ou equipes de operações que usam software e automação para solucionar problemas e gerenciar sistemas de produção.

O que faz um engenheiro de confiabilidade de sites?

A função do engenheiro de confiabilidade de sites é singular e requer experiência com administração de sistemas, desenvolvimento de software com uma base adicional em operações ou alguém em uma função de operações de TI que também tenha habilidades de desenvolvimento de software.

DevOps x SRE

A metodologia DevOps é uma abordagem de cultura, automação e design de plataforma que tem como objetivo agregar mais valor aos negócios e aumentar a capacidade de resposta às mudanças por meio de entregas de serviços rápidas e de alta qualidade. A SRE pode ser considerada uma forma de implementar a metodologia DevOps. Assim como o DevOps, a SRE tem como foco a cultura e os relacionamentos. Ambas as abordagens têm como objetivo aproximar as equipes de operações e desenvolvimento para acelerar a entrega de serviços. Ao codificar e criar novas funcionalidades, o DevOps se concentra em percorrer o pipeline de desenvolvimento de modo eficiente. Já a abordagem de SRE se concentra no equilíbrio entre os esforços de manter a confiabilidade de sites e a criação de novas funcionalidades.

Differences Between DevOps & SRE

DevOps

1. Focus is on the software core development.
2. Team members are development-oriented but are informed of the needs of the operations team.
3. Works with the operations team to assist in preparing the software for operations.

SRE

1. Focus is on response times and software reliability.
2. Team members are operations-oriented but are informed on the needs of the development team.
3. Works with the development team to assist in informing them on the needs of the operations team.





PUC Minas
Virtual

Application Performance Management (APM)

Application Performance Management

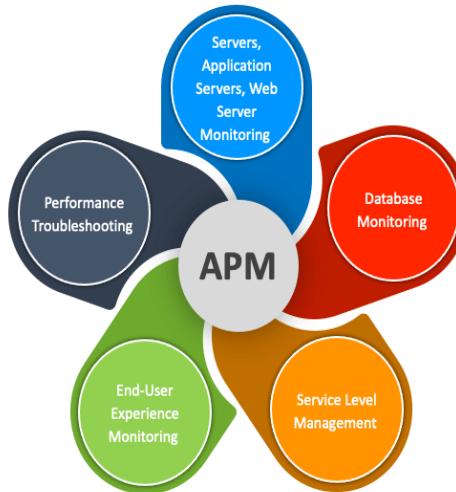
Também conhecido como Application Performance Management, o APM é um tipo de software, ou até serviço, que se certifica se os softwares estão com o desempenho e performance adequada. Ele monitora a velocidade e a linearidade de transações digitais dos mais variados tipos: softwares, sistemas, infraestruturas de rede, etc. Por meio de testes de carga, monitoramento da experiência real de usuários, desempenho web, prevenção de erros e bugs e até instrumentalizando a aplicação, o APM é um tipo de solução muito adequada para auxiliar empresas que possuem sistemas desenvolvidos **internamente ou possuem grandes desafios relacionados a infraestruturas complexas**. O resultado alcançado por isso, deve ser uma boa experiência final para o usuário.

Observabilidade – Como medir

Dimensões serviços de APM

APPLICATION PERFORMANCE MANAGEMENT

Solução de problemas



End user experience (Experiência do usuário final)

O monitoramento da experiência do usuário final pode ser realizada de duas maneiras: sintética/proativa ou real. A mais comum é a sintética/proativa, que é feita via robôs emuladores, que simulam o comportamento do usuário na forma real, por meio de logs de aplicação ou plugins de softwares especializados em APM. Nos dois tipos a monitoração é utilizada para gerar dashboards e disparar alarmes, caso ocorra alguma violação de tempo ou SLA.

Runtime application architecture (Arquitetura do aplicativo e tempo de execução)

O uso do runtime application architecture para conhecer o fluxo das transações é de extrema importância, pois cada vez mais as aplicações se encontram distribuídas e descentralizadas. Ter um desenho transacional atualizado de forma automática, faz parte da entrega de algumas das muitas ferramentas de APM do mercado.

Deep Dive Component Monitoring(Monitoramento de componentes de mergulho profundo)

O uso do runtime application architecture para conhecer o fluxo das transações é de extrema importância, pois cada vez mais as aplicações se encontram distribuídas e descentralizadas. Ter um desenho transacional atualizado de forma automática, faz parte da entrega de algumas das muitas ferramentas de APM do mercado.

Analytics/Reporting(Análise/Relatórios)

Normalmente, após a coleta de dados diretamente nas aplicações e infraestruturas que as sustentam, as soluções de APM fornecem ferramentas para analytics e reporting. Nesse caso, dados brutos são coletados para uma posterior análise acerca do desempenho, capacidade ou custos (caso em cloud) de uma aplicação.

Analytics/Reporting(Análise/Relatórios)

Normalmente, após a coleta de dados diretamente nas aplicações e infraestruturas que as sustentam, as soluções de APM fornecem ferramentas para analytics e reporting. Nesse caso, dados brutos são coletados para uma posterior análise acerca do desempenho, capacidade ou custos (caso em cloud) de uma aplicação.

APPLICATION PERFORMANCE MANAGEMENT

APM Service Offerings





PUC Minas
Virtual

Elementos da monitoração

Network Performance Monitor

O Network Performance Monitor é um de monitoramento de rede avançado e acessível que permite detectar, diagnosticar e resolver rapidamente problemas de desempenho e falhas de rede, permite que os usuários se conectem a dados de aplicativos, de servidor, virtuais e correlacionem esses dados para diagnosticar e resolver problemas de desempenho complexos da rede híbrida.

Network Performance Monitor

Por meio de integrações profundas com produtos, permite unir silos de domínios para executar a análise de causa raiz rapidamente com ferramentas detalhadas e Mapas , permitindo que os usuários obtenham insights de dados correlacionados historicamente e em tempo real.

Network Performance Monitor

Permite criar uma central de mensagens compartilhada na qual é possível ver eventos e alertas na sua rede em uma única visualização, além de mecanismos de escalabilidade e insights de dispositivos avançados para solucionar problemas. O Network Performance Monitor é um processo de monitoramento de rede avançado e acessível que permite detectar, diagnosticar e resolver rapidamente problemas de desempenho e falhas de rede.

Analise de Trafego

O Analisador de tráfego é um processo complementar que permite que ferramentas analisem fluxos de vários fornecedores afim de reduzir proativamente o tempo de inatividade da rede. A análise de tráfico fornece insights que podem ser colocados em prática para ajudar os profissionais de TI a solucionar problemas e otimizar o consumo de largura de banda. Esses insights indicam quem e o que consome tráfego e onde o tráfego é consumido.

Analise de Trafego

Na analise de trafego utilizamos infraestruturas modulares para facilmente integrar e detectar dados . Por meio de integrações profundas e com base na analyses produtos, como uma central de mensagens compartilhada na qual é possível ver eventos e alertas na sua rede em uma única visualização para solucionar problemas rapidamente em toda a plataforma.

Gestão dos Endereços de IP

Uma grande parte de ter de lidar com as redes e os desafios complexos da rede atual começa com o gerenciamento do inventário de endereços IP e de recursos essenciais de DNS e DHCP. Você pode criar acesso ao gerenciamento centralizado de endereços IP, pois ele atua com a administração unificada de DHCP e DNS e ajuda as equipes a encontrar e configurar endereços disponíveis em sistemas DHCP e DNS.

Gestão dos Endereços de IP

- Crie e mantenha grupos de IP e utilize-os em todos para caracterizar o tráfego entre grupos e definir aplicativos personalizados.
- Personalize alertas quando houver conflito de IPs e acelere a resolução de conflitos de endereços IP com o ferramentas para identificar a causa raiz por endereço MAC, fornecedor, porta de switch, SSID Wi-Fi e usuário.
- Visualize todos os eventos e alertas na sua rede de uma só vez para solucionar problemas de dispositivos avançados em toda a plataforma de monitoramento e obeservabilidade.

User Device

Controle automatizado de usuários e dispositivos, juntamente com recursos avançados de gerenciamento de porta de switch para que você possa controlar quem ou o que se conecta à sua rede. Localize rapidamente um computador ou usuário e rastreie dispositivos perdidos ou invasores com uma simples busca pelo nome de usuário, endereço IP, nome do host ou endereço MAC.

- Oferece informações sobre aumento de largura de banda do usuário e localização da porta de switch, permitindo que você reduza o uso de largura de banda ou remova-a da rede.
- Simplifica e acelera a resolução de conflitos de IP ao permitir que usuários identifiquem um problema, recebam alertas em caso de conflito e desativem a causa remotamente.

Não deixe que aplicativos lentos e tempos de inatividade afetem os usuários finais e os serviços de sua empresa. Identifique a causa raiz de problemas de aplicativos em várias camadas da pilha de TI. Descubra automaticamente o ambiente do seu aplicativo e comece a monitorar em apenas uma hora.

- Para ver o desempenho, o tempo de atividade, a capacidade e a utilização de recursos em toda a pilha de TI(lista de softwares, estruturas, tecnologias, linguagens de programação etc).
- Certifique-se de que os problemas de configuração não estão afetando o desempenho dos sistemas e aplicativos.

Configuração de Servidores

Quando as configurações começam a perder o rumo, o impacto pode ser grave: interrupções, lentidão e violações de segurança e conformidade. As ferramentas de monitoramento podem revelar rapidamente quando as configurações do servidor, aplicativo ou banco de dados mudarem, quem as está mudando, o que mudou e qual o impacto para o desempenho. Isso ajudará você a ter a visibilidade necessária para solucionar problemas mais rápido, melhorar a segurança e demonstrar conformidade.

Configuração de Servidores

Quando as configurações começam a perder o rumo, o impacto pode ser grave: interrupções, lentidão e violações de segurança e conformidade. As ferramentas de monitoramento podem revelar rapidamente quando as configurações do servidor, aplicativo ou banco de dados mudarem, quem as está mudando, o que mudou e qual o impacto para o desempenho. Isso ajudará você a ter a visibilidade necessária para solucionar problemas mais rápido, melhorar a segurança e demonstrar conformidade.

Configuração das Virtualizações

O gerenciamento de desempenho, o planejamento de capacidade e a otimização entre ambientes VMware vSphere, Microsoft Hyper-V e Nutanix AHV.

- Identificar se a lentidão é causada por um aplicativo, servidor virtual, host ou repositório de dados.
- Recomendações de desempenho ativas e preditivas e leve as métricas básicas de desempenho de VM disponíveis.
- Visibilidade de seu desempenho de ambiente virtual VMware, Hyper-V e Nutanix no VMAN (além do monitoramento de hosts físicos) para identificar e resolver problemas mais rápido.

Performance Web

Monitorar a experiência do usuário e avaliar as transações de sites internos e externos e aplicativos baseados na Web – em qualquer local. Você pode identificar rapidamente elementos que apresentam lentidão ou falhas e solucionar os problemas até a infraestrutura de suporte, do servidor da Web e do banco de dados até o hardware de armazenamento:

- Veja a experiência do usuário final, além das métricas de rede e sistemas para identificar e entender o escopo dos problemas.
- Use o mecanismo de alertas inteligentes para criar alertas personalizáveis em um só lugar, definir critérios de notificação, acionar scripts externos e integrar-se aos sistemas de emissão de tíquetes do Service desk .

Analise do Logs

Com a coleta, análise e visualização de logs em tempo real, você obtém visibilidade pronta para uso do desempenho e da disponibilidade de sua infraestrutura e aplicativos de TI:

- Visualize os dados de log e o desempenho de rede e sistemas facilmente para acelerar a solução de problemas com integração total de dados de logs e eventos.
- Colete, consolide e analise os eventos de rede, sistemas, Windows e VMware, juntamente com dados de desempenho e disponibilidade .

Aplicabilidade

É aconselhável ter um APM se:

- Sua organização desenvolve aplicativos do zero
- Sua receita depende das aplicações desenvolvidas
- Você possui vários sistemas que interagem ou dependem de outras aplicações
- As operações de negócios dependem das aplicações desenvolvidas internamente
- A aplicação depende do suporte regular de um fornecedor e você depende dos membros internos da equipe de TI para apoiá-la



PUC Minas
Virtual

Data Observability

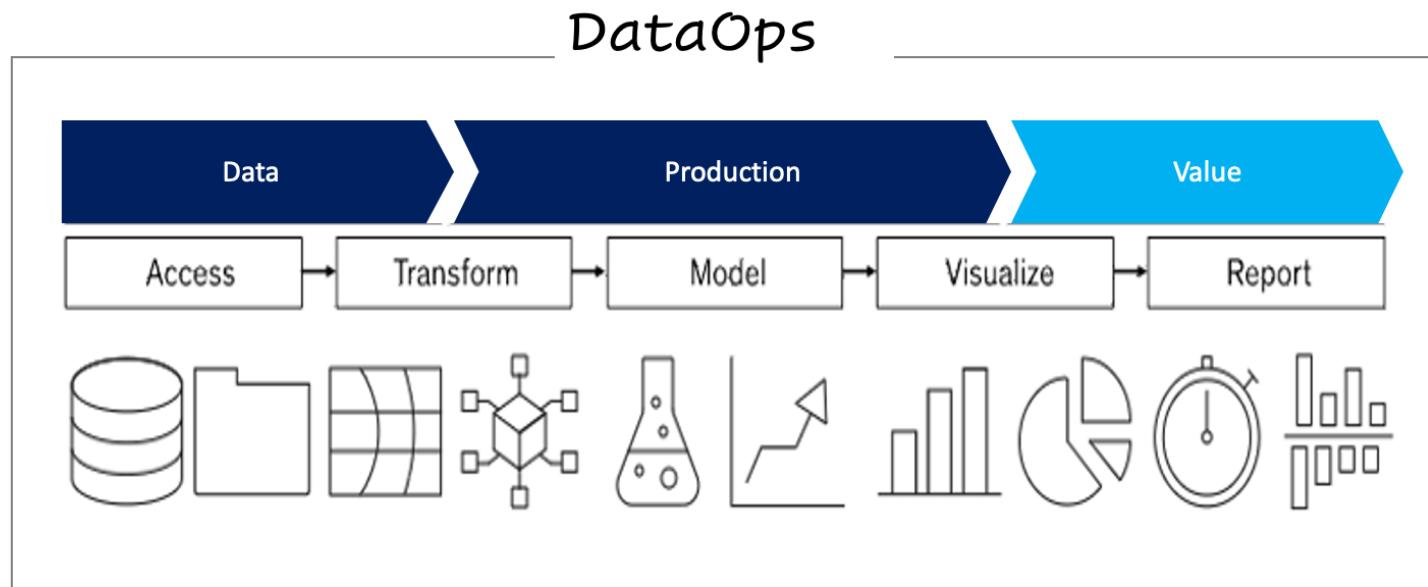
Observabilidade dos dados

A observabilidade de dados (Data Observability) refere-se à capacidade de coletar e analisar dados para entender e otimizar o desempenho de um sistema. Os dados se tornaram um dos ativos mais valiosos dos tempos modernos. À medida que mais empresas dependem de insights de dados para conduzir decisões críticas de negócios, os dados devem ser precisos, confiáveis e de alta qualidade.

Observabilidade dos dados

Um aspecto fundamental da observabilidade de dados é a capacidade de acessar e analisar dados de todas as partes do sistema. Isso inclui dados de aplicações, da infraestrutura e dos usuários do sistema. Ao coletar dados de todas essas fontes, é possível obter uma visão completa do sistema e identificar áreas de melhoria. Outro aspecto importante da observabilidade de dados é a capacidade de identificar e solucionar problemas em tempo real. Ao monitorar constantemente os dados, é possível detectar e resolver problemas antes que eles se tornem críticos.

Observabilidade dos dados





PUC Minas
Virtual

Estudos

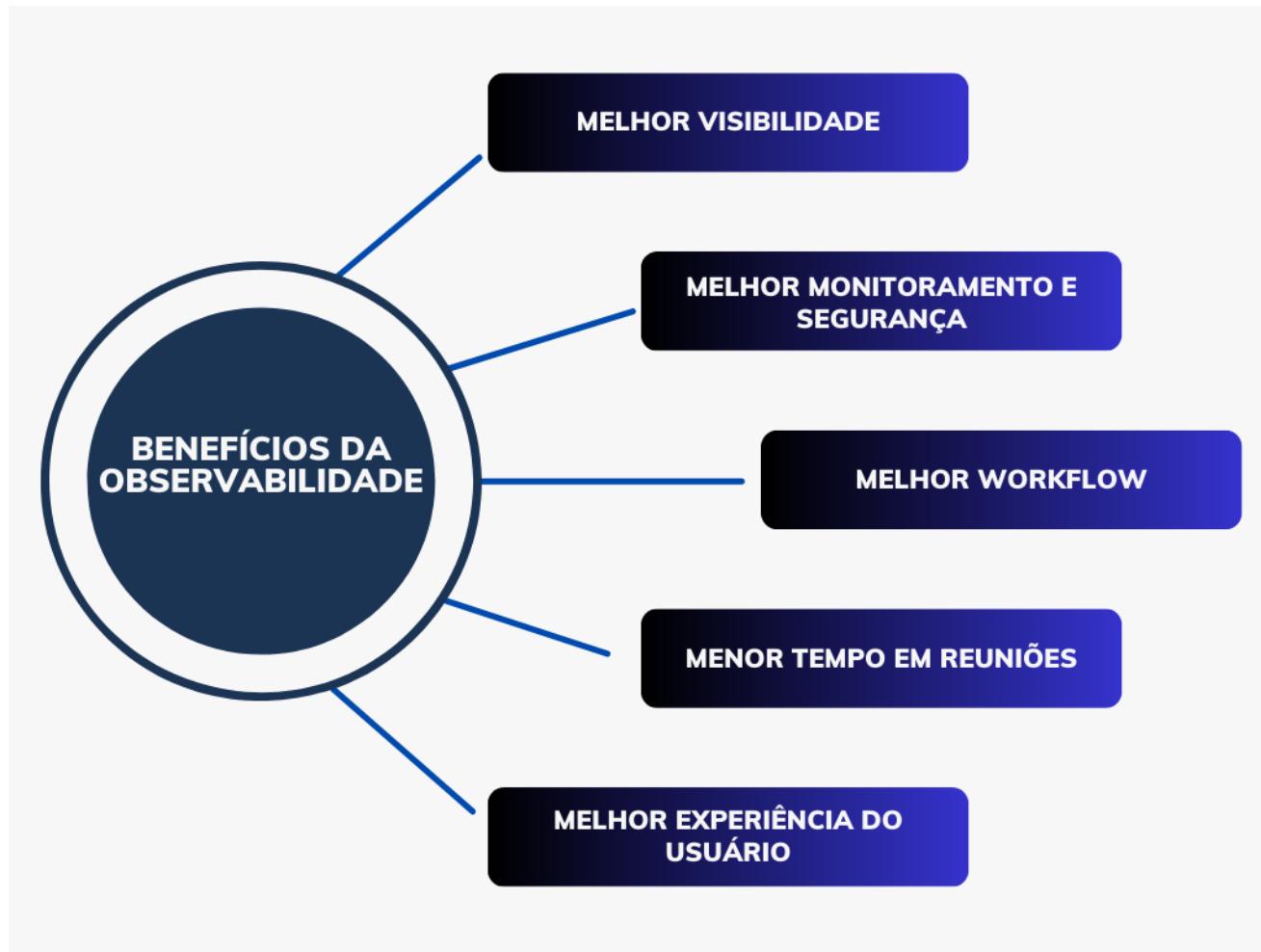
Estudos mostram que 78% dos clientes desistem de uma compra devido a uma experiência insatisfatória.

Indisponibilidade do sistema: Sem a observabilidade adequada, é difícil identificar problemas que possam estar causando a indisponibilidade do seu sistema, como problemas de recursos, falhas de hardware ou problemas de software. Isso pode resultar em períodos de inatividade e interrupções no negócio.

Problemas de segurança: Sem informações detalhadas sobre o comportamento de um sistema, é difícil identificar e corrigir problemas de segurança, como vulnerabilidades, ataques de rede ou invasões. Isso pode resultar em danos aos dados ou a reputação da empresa.

Problemas de escalabilidade: Sem informações sobre o comportamento de um sistema, é difícil identificar pontos de gargalo ou limitações que possam estar impedindo o crescimento ou a escalabilidade do sistema. Isso pode resultar em perda de oportunidades de negócios e dificuldades para atender às demandas dos usuários.

Estudos



A Observabilidade Aplicada (Applied Observability) possui 3 elementos-chave: democratização dos dados, múltiplas camadas de dados simultâneas e implementação. Ao analisarmos esses três elementos, vemos que a maioria dos fornecedores já estão adotando a abordagem de que quanto mais dados observados, melhor o resultado da correlação. No entanto, penso que o maior desafio é a implementação, pois ela envolve estratégia e vários stakeholders. Juntamente a isso, um grande desafio que profissionais de observabilidade tem encontrado é levar a mensagem de que monitoramento e observabilidade andam juntos, mas são conceitos diferentes. Isso também vale outro post.

Gartner.

3 Key Elements of Applied Observability

The diagram consists of three horizontal grey boxes stacked vertically, each containing an orange icon and text. To the left of the boxes is a large orange number '3' followed by the text 'Key Elements of Applied Observability'. Above the first box is the Gartner logo. To the right of the boxes is a vertical stack of three orange icons: a central processing unit (CPU), two overlapping arrows (one pointing up, one pointing down), and a gear.

- Democratized opportunity
- Multiple concurrent data layers
- Implementation

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved.



PUC Minas
Virtual

Produto

Modelo

Ambiente de produção é, de longe, a parte mais importante e, surpreendentemente, menos discutida do Ciclo de Vida do Modelo. É aqui que o modelo atinge o negócio. É onde as decisões que o modelo toma realmente melhoram os resultados ou causam problemas para os clientes. Ambientes de treinamento do modelo, onde os Cientistas de Dados passam a maior parte de seu tempo, consistem em apenas uma amostra do que o modelo verá no mundo real. Em um ambiente de desenvolvimento de software bem controlado, um engenheiro tem controle de versão, análise de cobertura de teste, teste de integração, testes executados em check-ins de código, revisões de código e reproduzibilidade.

Validação

Os modelos são construídos e avaliados usando vários conjuntos de dados. O conjunto de dados de treinamento é usado para ajustar os parâmetros do modelo. O conjunto de dados de validação é usado para avaliar o modelo durante o ajuste de hiperparâmetros.

Validação

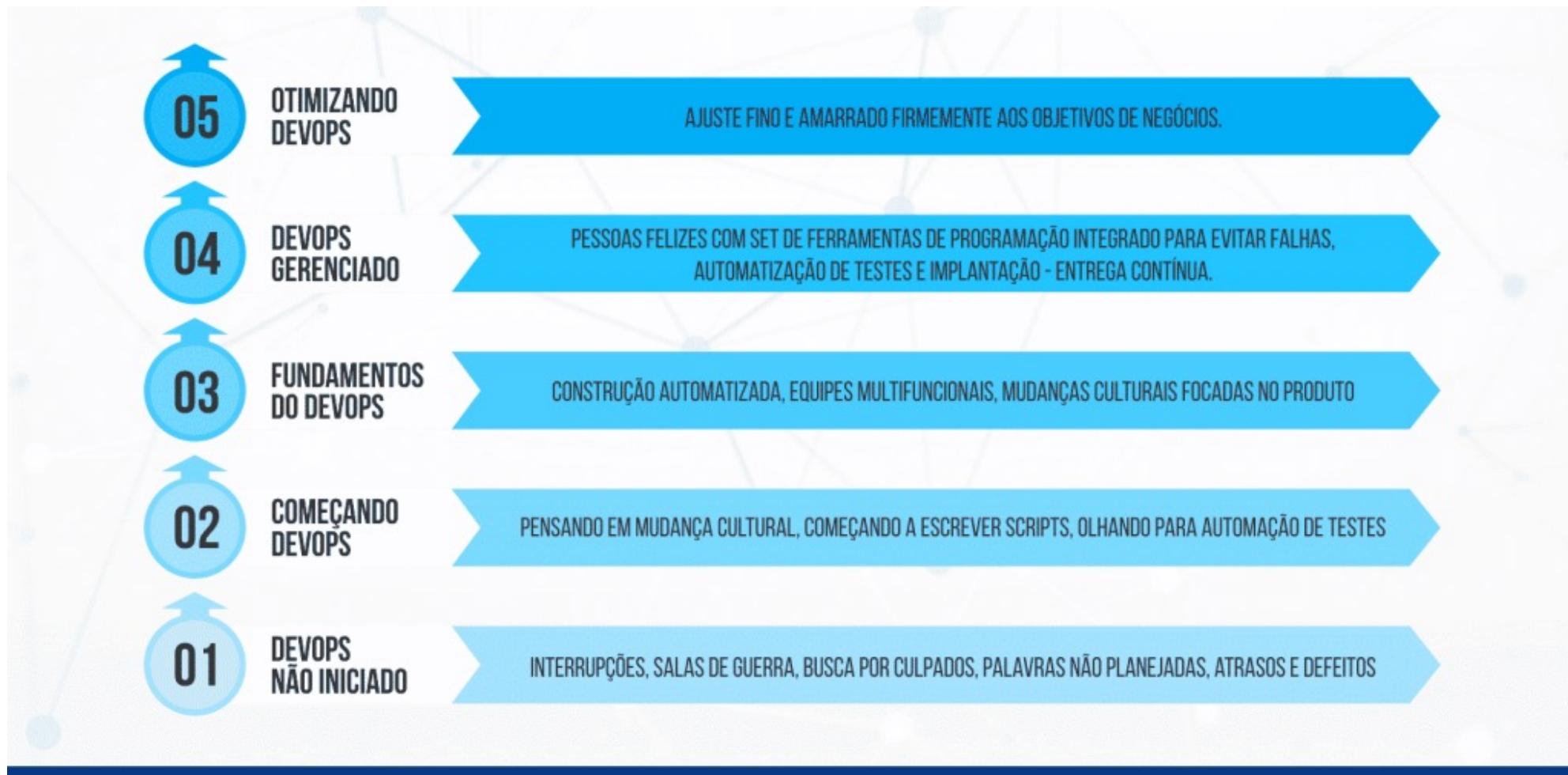
Independentemente do setor, há certas verificações a serem feitas antes de implantar o modelo na produção. Essas verificações incluem (mas não estão limitadas a):

- Testes de avaliação de modelo (precisão), tanto no geral como por fatia.
- Verificações de distribuição de previsão para comparar a saída do modelo com as versões anteriores.
- Verificações de distribuição de recursos para comparar recursos altamente importantes com testes anteriores.

Validação

- Análise de importância de recursos para comparar mudanças em recursos que estão sendo usados para decisões.
- Análise de sensibilidade para ruído de entrada aleatório e extremo.
- Teste de estresse do modelo.
- Viés e Discriminação.
- Erro de rotulagem e verificações de qualidade de recursos.
- Verificações de vazamento de dados.
- Verificações de ajuste excessivo e insuficiente.
- Dados históricos para comparar e avaliar o desempenho.
- Testes de pipeline de recursos que garantem que não haja quebra de recurso entre pesquisa e produção.

Validação



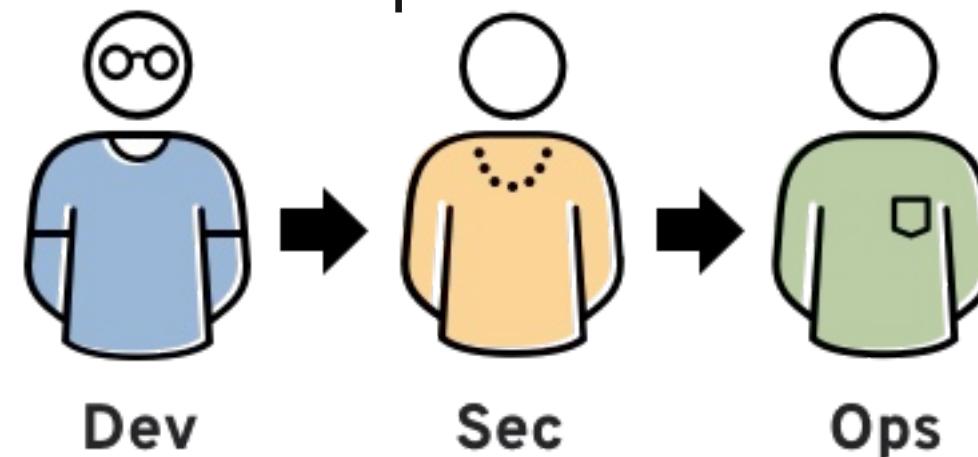


PUC Minas
Virtual

DevSecOPS

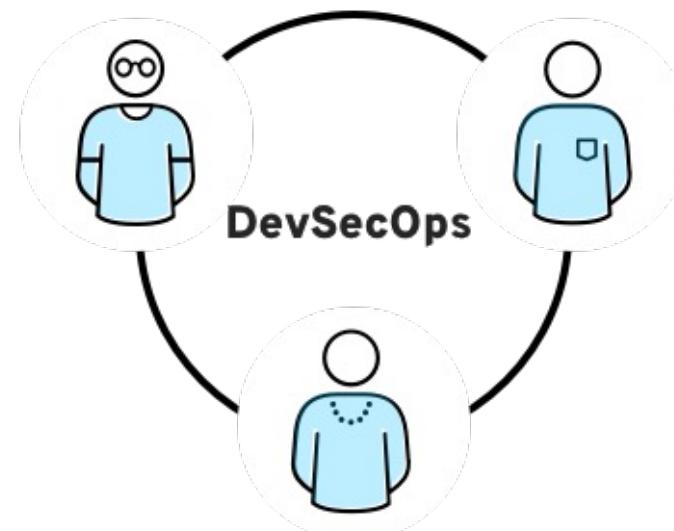
DevSecOps significa desenvolvimento, segurança e operações. É uma abordagem à cultura, automação e design da plataforma que integra segurança ao DevOps como uma responsabilidade compartilhada em todo o ciclo de vida da TI.

A metodologia DevOps não envolve apenas as equipes de desenvolvimento e de operações. Se você quiser aproveitar ao máximo a agilidade e a capacidade de resposta proporcionadas pela abordagem DevOps, também será necessário que a equipe de segurança da TI desempenhe um papel integrado em todo o ciclo de vida das aplicações da sua empresa.



DevSecOps

Agora, no framework colaborativo do DevOps, a segurança é uma responsabilidade compartilhada e integrada do início ao fim. É uma mentalidade tão importante que resultou na criação do termo "DevSecOps" para enfatizar a necessidade de criar uma base de segurança para sustentar as iniciativas de DevOps.



Segurança automatizada

O que é preciso fazer: manter os ciclos de desenvolvimento curtos e frequentes, integrar as medidas de segurança com mínima interrupção das operações, acompanhar o ritmo das tecnologias inovadoras (como containers e microserviços) e, acima de tudo, estimular a colaboração entre equipes que normalmente trabalham isoladas, uma tarefa complicada em qualquer organização. No entanto, o elemento facilitador dessas mudanças no aspecto humano do framework de DevSecOps é a automação.



Segurança para ambientes e dados

- **Padronize e automatize o ambiente:** cada serviço deve ter o mínimo possível de privilégios para reduzir as conexões e os acessos não autorizados.
- **Centralize os recursos de controle de acesso e identidade de usuários:** ter um controle rígido do acesso e usar mecanismos de autenticação centralizados são fatores essenciais para a segurança dos microsserviços, já que a autenticação é iniciada em vários pontos.
- **Isole os containers que executam microsserviços um dos outros e da rede:** isso inclui dados em trânsito e em repouso, já que ambos os tipos podem ser alvos de ataques.
- **Criptografe os dados trocados entre aplicações e serviços:** uma plataforma de orquestração de containers com funcionalidades de segurança integradas ajuda a minimizar a chance de ocorrerem acessos não autorizados.
- **Introduza gateways de API seguros:** APIs seguras aumentam a visibilidade de autorização e roteamento. Ao diminuir a quantidade de APIs expostas, as organizações podem reduzir as superfícies de ataque.

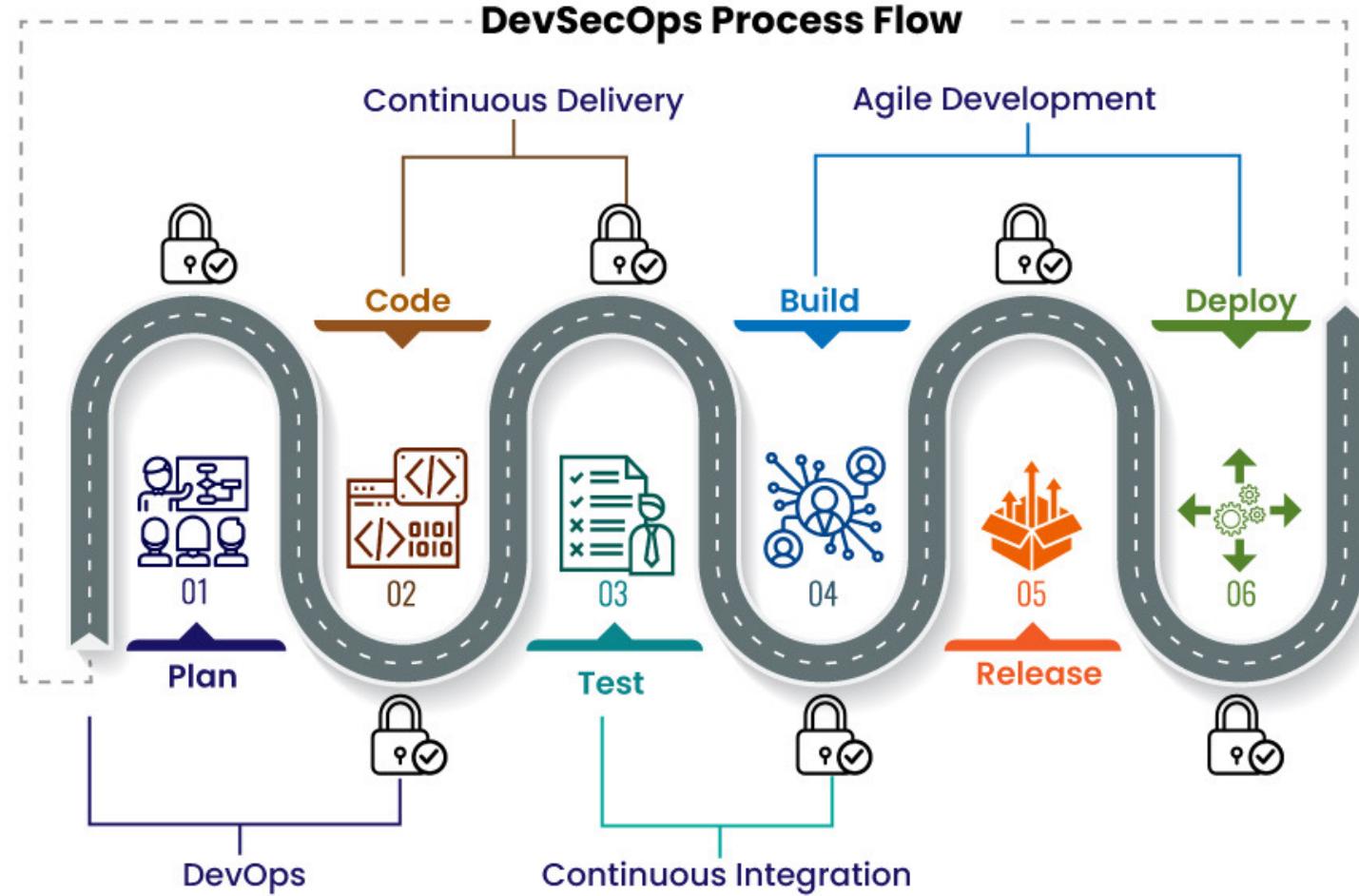
Segurança do processo de CI/CD

- **Integre verificadores de segurança para containers:** isso deve fazer parte do processo de inclusão de containers no registro.
- **Automatize os testes de segurança no processo de integração contínua:** isso inclui executar ferramentas de análise estática de segurança como parte das compilações, bem como verificar quaisquer imagens de container criadas anteriormente para encontrar vulnerabilidades de segurança conhecidas conforme elas são inseridas no pipeline de criação.
- **Adicione testes automatizados para os recursos de segurança no processo de teste de aceitação:** automatize os testes de validação de entradas e os funcionalidades de autorização e autenticação da verificação.

Segurança do processo de CI/CD

- **Automatize as atualizações de segurança, como patches, para identificar vulnerabilidades conhecidas:** faça isso por meio de um pipeline DevOps. Essa medida deve eliminar a necessidade de administradores se conectarem aos sistemas de produção, a mesmo tempo que cria um log de alterações rastreáveis e documentadas.
- **Automatize os recursos de gerenciamento das configurações de serviços e sistemas:** com isso, é possível manter a conformidade com as políticas de segurança e eliminar os erros manuais. As tarefas de auditoria e correção também devem ser automatizadas.

Segurança do processo de CI/CD





PUC Minas
Virtual

ITSM

Gerenciamento de Serviços de TI

Uma ferramenta de ITSM pode executar várias funções, como gerenciamento de incidentes, gerenciamento de solicitações de serviço, gerenciamento de problemas e gerenciamento de mudanças, apenas para citar algumas. Uma ferramenta de ITSM geralmente também consiste também de um CMDB.

Gerenciamento de Serviços de TI

Information Technology Service Management – em português “Gerenciamento de Serviços de TI” – ou somente a sigla ITSM é um processo de gerenciamento indispensável para o ciclo de vida do TI, tão essencial na interligação de tantos setores de uma empresa.

Através do ITSM, gerenciar a definição e implementação de processos, criar estratégias de melhoria contínua para os serviços e servidores e acompanhar o cumprimento de normas e valores em uma empresa tornam-se mais fáceis. O ITSM transforma o TI em um sistema integrado a todas as atividades da empresa, e permite uma abordagem mais focada nos clientes e nos serviços de TI voltados para o cliente, como o suporte, sempre priorizando o melhor caminho.

Como funciona o ITSM?

O ITSM possibilita a integração de aspectos tecnológicos de diversos setores de uma empresa, como marketing, finanças e recursos humanos, facilitando a identificação de informações, a identificação de problemas e consertando falhas. Geralmente o gerenciamento de nível de serviços de TI na prática acontece seguindo as seguintes estratégias:

- Mapeamento e inventário da infraestrutura de TI da empresa;
- Avaliação sobre os serviços de TI, equipamentos e outras ferramentas tecnológicas que podem auxiliar o negócio;
- Análise e interação com outras áreas da empresa, podendo tornar o projeto mais consistente;
- Definição de cronograma e metas de reestruturação, respeitando as prioridades e custos;
- Monitoramento e avaliação dos resultados constantemente.

Como realizar o gerenciamento de serviços de TI

O gerenciamento de serviços de TI na prática envolve alguns passos fundamentais. Confira abaixo quais são eles:

- Tenha um plano estratégico de TI – esse plano estratégico pode seguir as mesmas normas do planejamento estratégico corporativo da empresa;
- Tenha um catálogo de serviços de TI – quais os principais serviços que a área de TI da sua empresa cobre?;
- Estabeleça metas de níveis de serviço (SLA) – que condições os serviços precisam ter para atingir as expectativas dos clientes?;
- Gerencie os incidentes – sempre que houver uma interrupção, queda de qualidade ou indisponibilidade de internet, é preciso estar preparado;

Como realizar o gerenciamento de serviços de TI

- 1.Gerencie os problemas – quais os sintomas causados pelos incidentes? Como gerenciar?;
- 2.Gerencie os projetos de TI – siga as melhores práticas mundiais, e tenha um portfólio de projetos;
- 3.Melhore os serviços de TI – avalie os serviços com frequência para detectar a necessidade de mudanças;
- 4.Gerencie a capacidade do serviço – qual a capacidade máxima de atendimentos que seu negócio consegue realizar?

Como realizar o gerenciamento de serviços de TI



Fonte de imagem : www.google.com



PUC Minas
Virtual

SIEM

5 exemplos de Gerenciamento de Serviços de TI

O SIEM, ou Gerenciamento de Informações e Eventos de Segurança em português, é a combinação do SEM (*Security Event Manager* - Gerenciamento de Eventos de Segurança) e SIM (*Security Information Management* - Gerenciamento de Informações de Segurança). Essa junção permite:

- Análise em tempo real de alertas de segurança;
- Comparação de eventos nos sistemas com as políticas de segurança para identificar ameaças avançadas;
- Gerenciamento de logs;
- Visão ampla e registros das atividades no ambiente de TI.

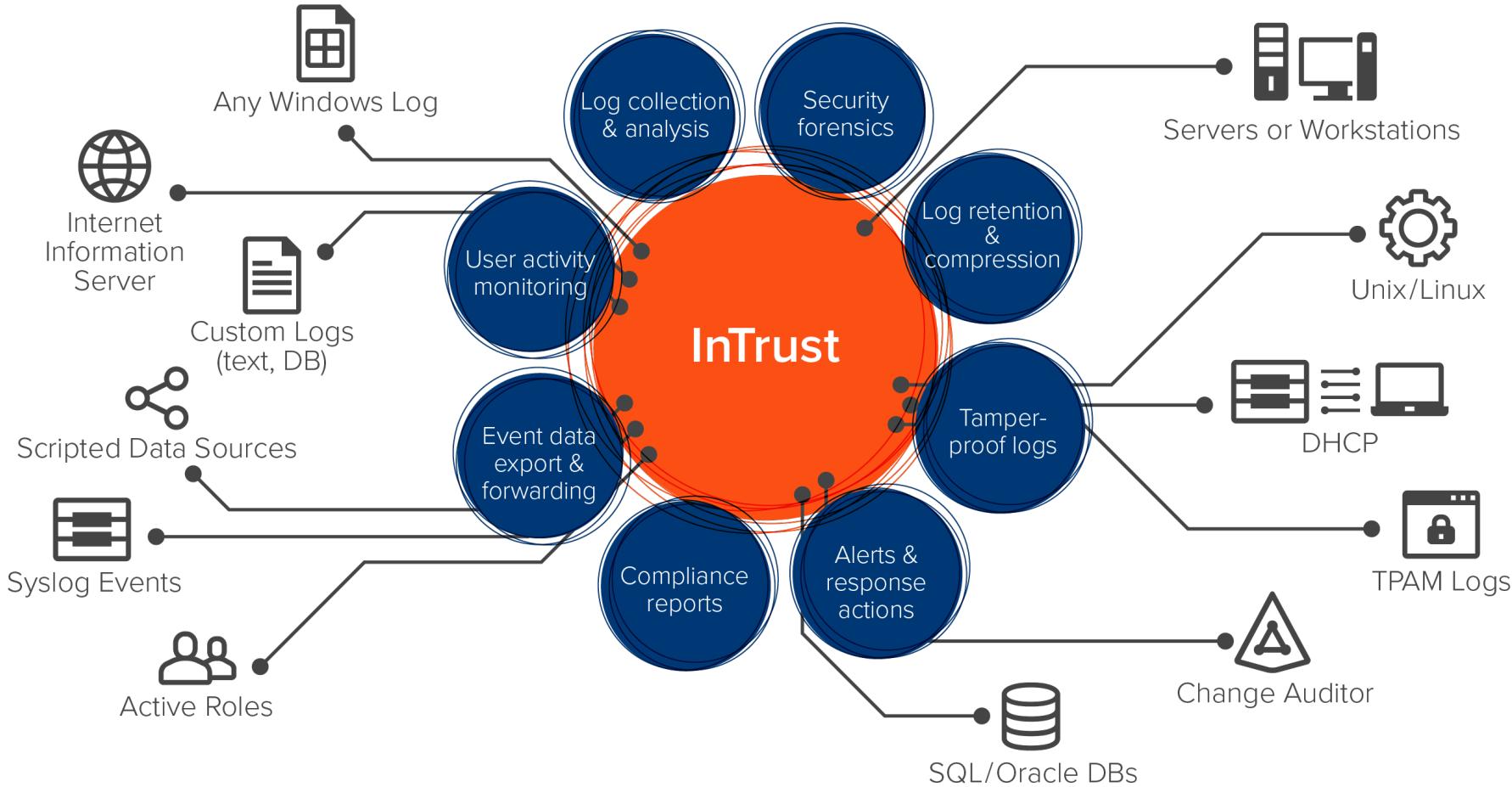
Como funciona o SIEM?

O SIEM coleta dados de diferentes fontes:

- Logs de firewall;
- Eventos gerados por aplicativos (por exemplo, antivírus);
- Dispositivos de segurança;
- Sistemas Host;
- E outros locais.

A partir disso, ele categoriza cada um desses dados. Então, quando o SIEM identifica uma ameaça, ele a classifica em um determinado nível - de acordo com as regras de segurança já pré-estabelecidas - e emite um alerta.

Como funciona o SIEM?





PUC Minas
Virtual