WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

Monitoramento de ativos de rede com ferramentas de código aberto

Ibirisol Fontes e Jundai Abdon

PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos

Introdução

- Sistemas computacionais cada vez mais complexos e distribuídos
  - Arquitetura *multitier*
  - Distribuídos geograficamente (escala global)
- Problemas cada vez mais granulares e específicos de plataformas
  - Diversas(os) redes, serviços, sistemas, recursos
  - Diversos fornecedores/fabricantes (funcionalidades diferentes)
  - *Troubleshooting* especializado

Como estão indo nossos serviços?

Estão funcionais e disponíveis?

Estão entregando o esperado aos clientes?

Estão corretamente mensurados para as demandas (escalabilidade vs custos)?

Como devemos nos preparar/planejas para o futuro?

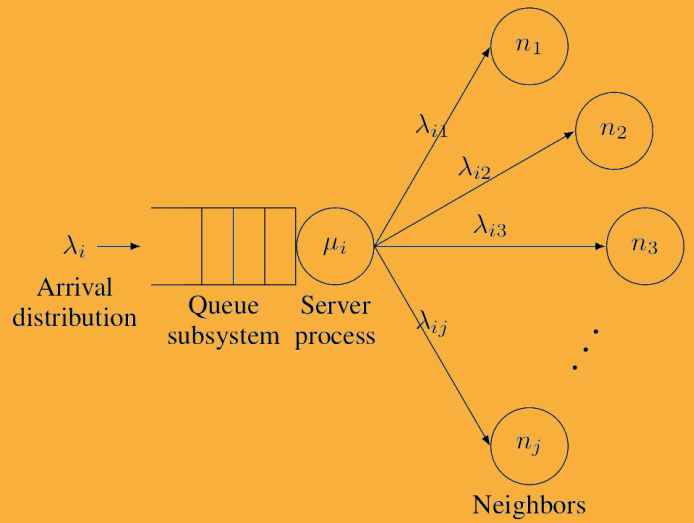
Quais serão as ações e diretrizes organizacionais?

Medição

- Mensurar, quantitativamente ou qualitativamente, o funcionamento de algo (elemento)
  - Teste de um sistema, componente, recurso, etc.
  - Teste em relação a capacidade, vazão, erro, corretude, etc.

Medição

- Sistemas de filas (Queueing theory)



* Imagem: *Um nó em um sistema de filas (queue model)*

Medição

- Formas de coleta do dados de um elemento
  - **Ativo** coletados pelo sistema de medição através da execução de uma rotina
  - **Passivo** coletados pelo sistema de medição através da observação do funcionamento
  - **In-Band** coletados por uma comunicação interna (através do próprio canal a ser medido)
  - **Out-of-Band** coletados por um canal de comunicação dedicado

Monitoramento

"A arte de armazenar medições, avaliar medições, apresentar medições, gerar utilidades para as medições, entre outras, por toda a vida útil de um sistema..."

* Fonte: *Analistas e operadores anônimos (AOA)*

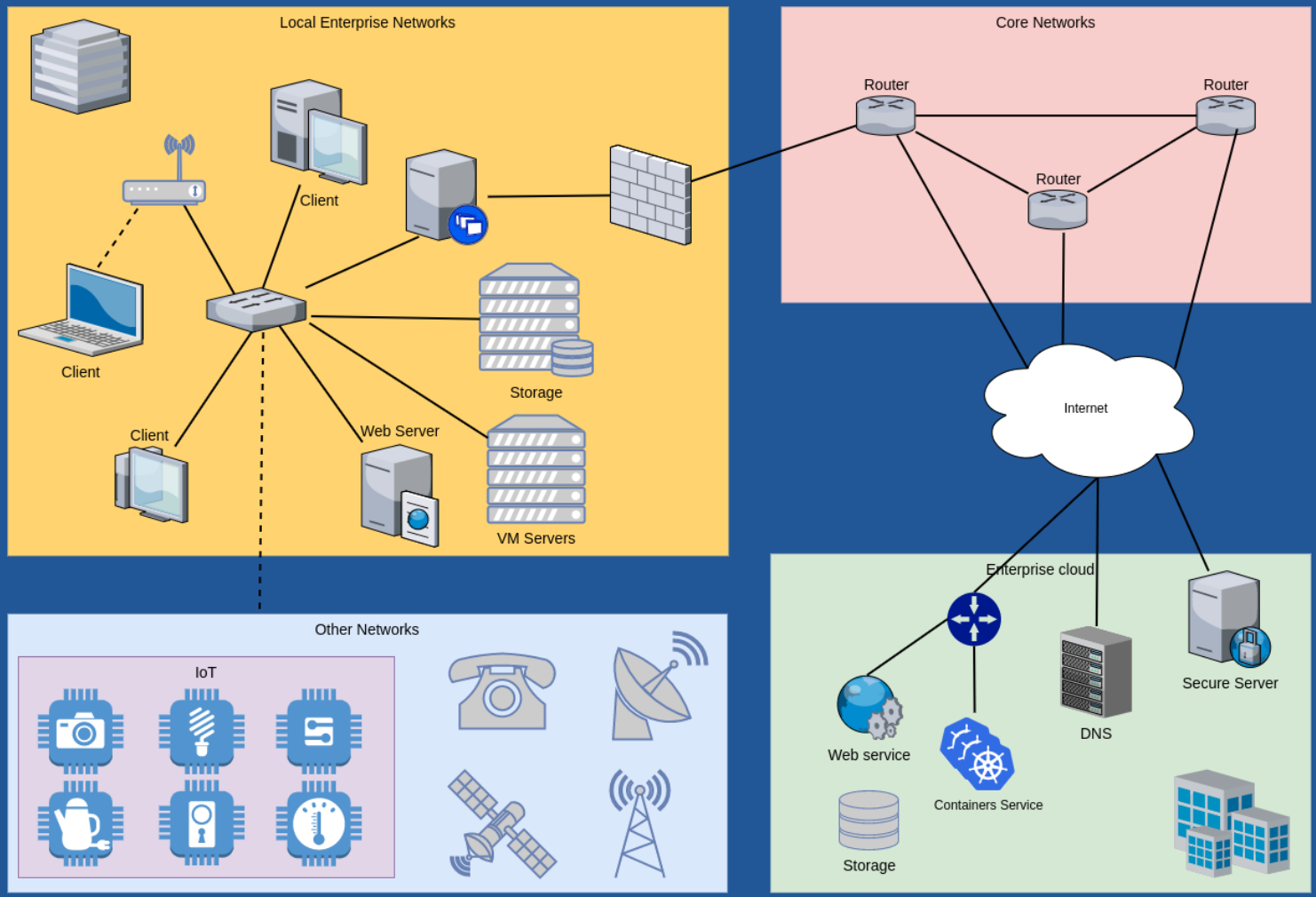
Monitoramento

- Entre os diversos tipos de monitoramento, utilização e performance são os mais comuns para visualização da saúde dos recursos de redes e sistemas de um determinado ambiente
- Diversas ferramentas e protocolos para tentar homogeneizar a aquisição de informações da infraestrutura
- Ferramentas voltadas para ambientes onde a visualização histórica de métricas é importante para planejamento e tomada de decisão na organização

Monitoramento

- Nem todas as soluções focam no armazenamento dessas métricas monitoradas de forma eficiente
- Normalmente há um superdimensionamento dos recursos necessários para um monitoramento completo de uma infraestrutura de TI

Monitoramento



* Imagem: *Infraestrutura de rede*

Monitoramento

- Visão sobre eventos de um sistema
- **Externa** através de checagens por entidades externas ao sistemas
  - *ping, telnet, ps, free, etc.*
- **Interna** através da exposição da saúde e performance das funções/componentes de um sistema
  - *snmp, sflow, telemetria, etc.*

Componentes

- **Métricas** Consolidação de requisições e recursos usados em um sistema, aplicação, equipamento, entre outras, em um determinado momento no tempo.

- **Logging** Registro detalhado de um evento em um sistema, contém informações de valores de variáveis e recursos associados ao evento em questão.

Componentes

- **Trace** Rastreamento de requisições em diversos subsistemas de um serviço/sistema a fim de registrar o ciclo de vida completo e identificar componentes que estejam gerando gargalos ou problemas.

- **Alerta** Validação de *thresholds* relacionados a métricas ou *logs* para geração de alertas aos administradores/operadores.

Modelo de coleta

- **Pull** Envio dos dados a partir de uma consulta do *sistema de monitoramento*
- **Push** Envio dos dados a partir de um eventos ou agendamento no *sistema monitorado*

Modelo de coleta

A coleta depende do sistema ou ativo a ser monitorado

- Forma de acesso
- Suporte de protocolos
- Recurso computacional (carga do monitoramento)
  - Dispositivos IoT (Gateways)

O que coletar? Quais métricas?

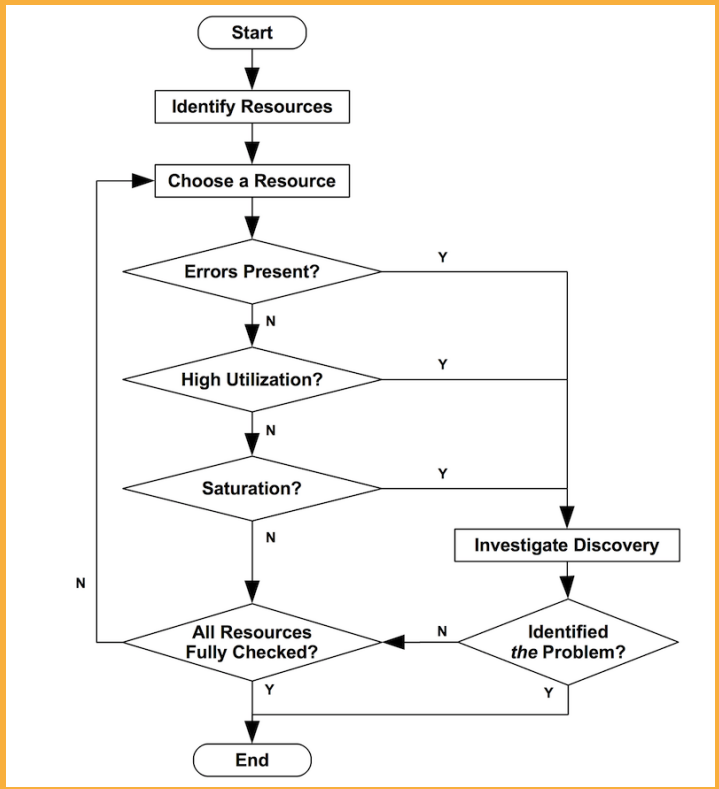
- Atraso de ida e volta (RTT – Round Trip Time)
- Erros de pacotes
- Utilização de banda
- Variação do atraso (jitter)
- Largura de banda alcançável (TCP, UDP)
- MOS (Mean Opinion Score)

O que coletar? Quais métricas?

- Fluxos de rede (volume de pacotes, bytes, tipo de protocolo, origens/destinos e portas)
- Status dos protocolos de roteamento
- Status e desempenho de serviços e aplicações
- Uso de recursos do sistema (CPUs, memória, disco, etc)
- Status e desempenho de máquinas físicas e virtuais

O que medir e monitorar?

- **Brendan Gregg's USE method (Utilization, Saturation, Errors)**



O que medir e monitorar?

- Baseado na visão de recurso (CPUs, disco, interfaces de rede, etc)
- **Utilização** média de ocupação de um recurso
- **Saturação** a medida pelo qual um recurso foi solicitado, mas estava ocupado (enfileiramento)
- **Errors** contagem de erros associados ao uso do recurso

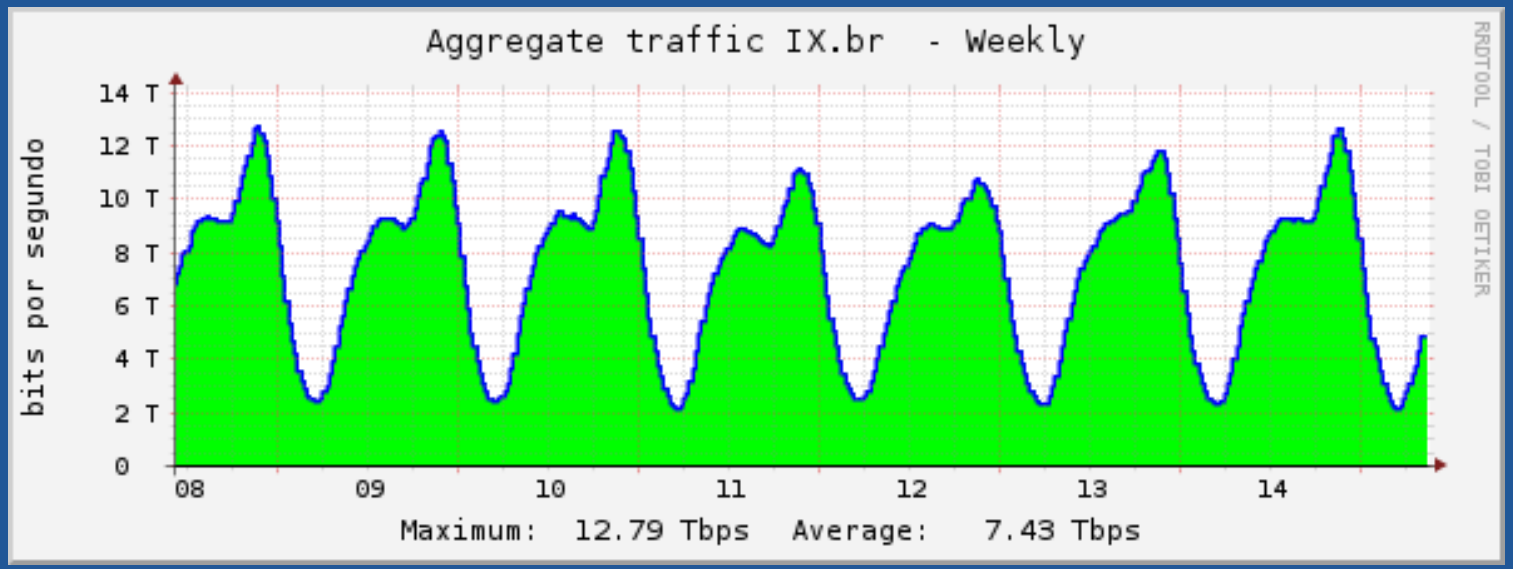
O que medir e monitorar?

- Brendan Gregg's USE method (Utilization, Saturation, Errors)
- **Tom Wilkie's RED method (Rate, Erros, Duration)**
- **Google's four golden signals (Latency, Traffic, Errors, Saturation)**

Temporalidade

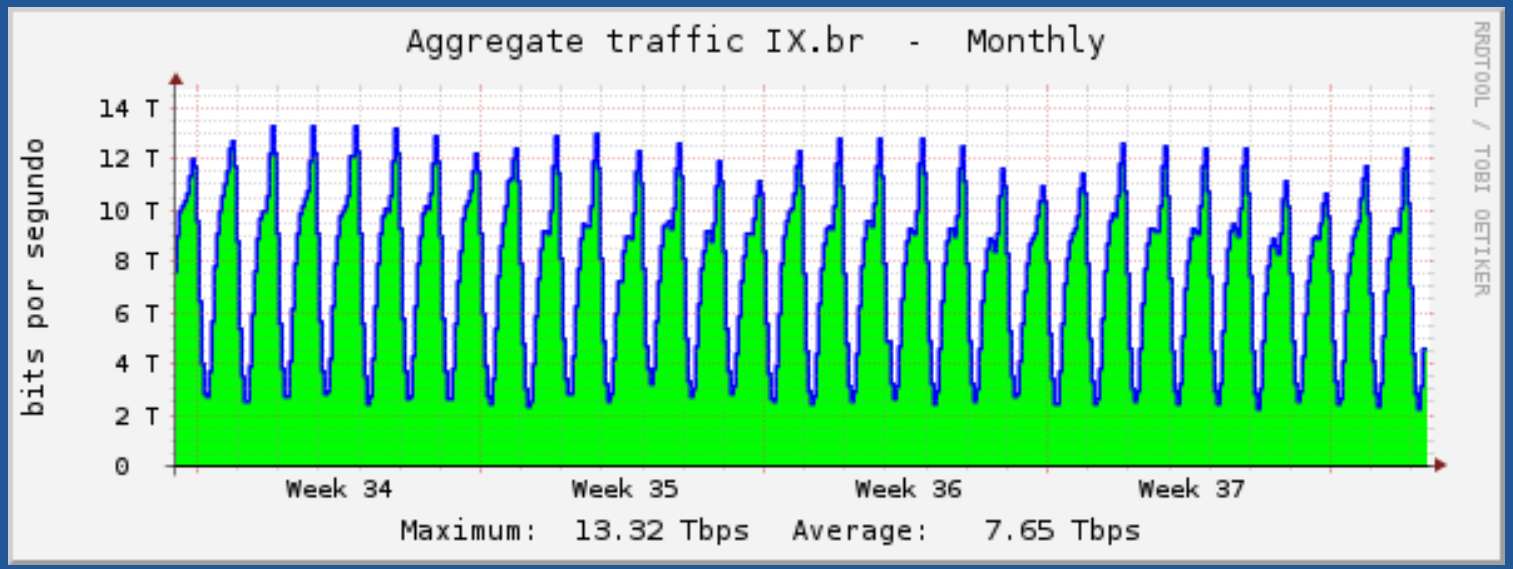
- Qual a granularidade da coletar?
- Quanto tempo devo armazenar?
- Qual a medida de armazenamento armazenar?

Temporalidade



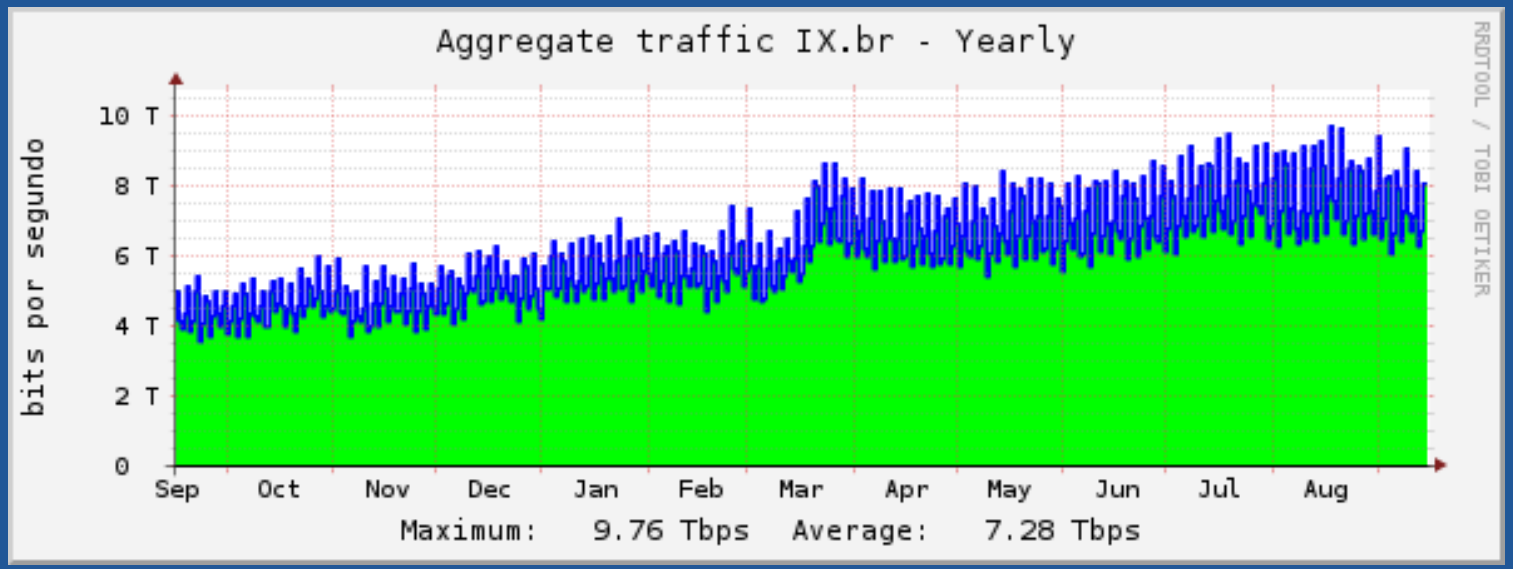
* Imagem: *Trafego IX.br (fonte: https://ix.br/agregado/)*

Temporalidade



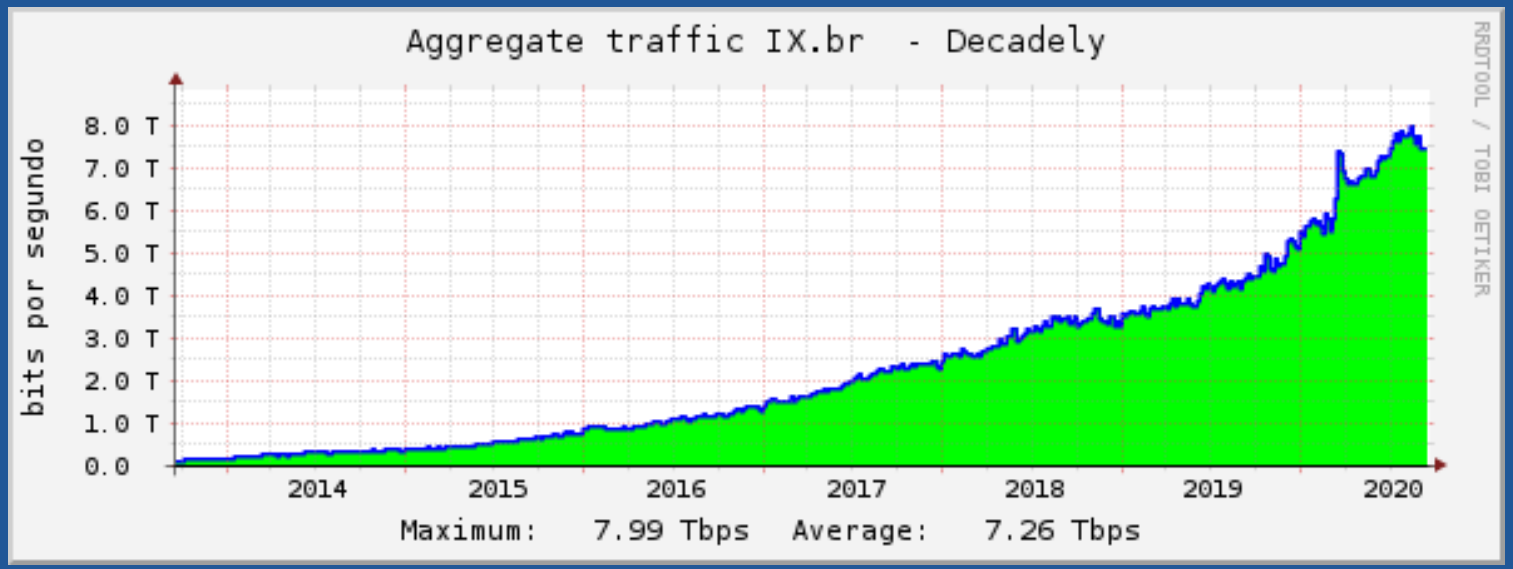
* Imagem: *Trafego IX.br (fonte: https://ix.br/agregado/)*

Temporalidade



* Imagem: *Trafego IX.br (fonte: https://ix.br/agregado/)*

Temporalidade



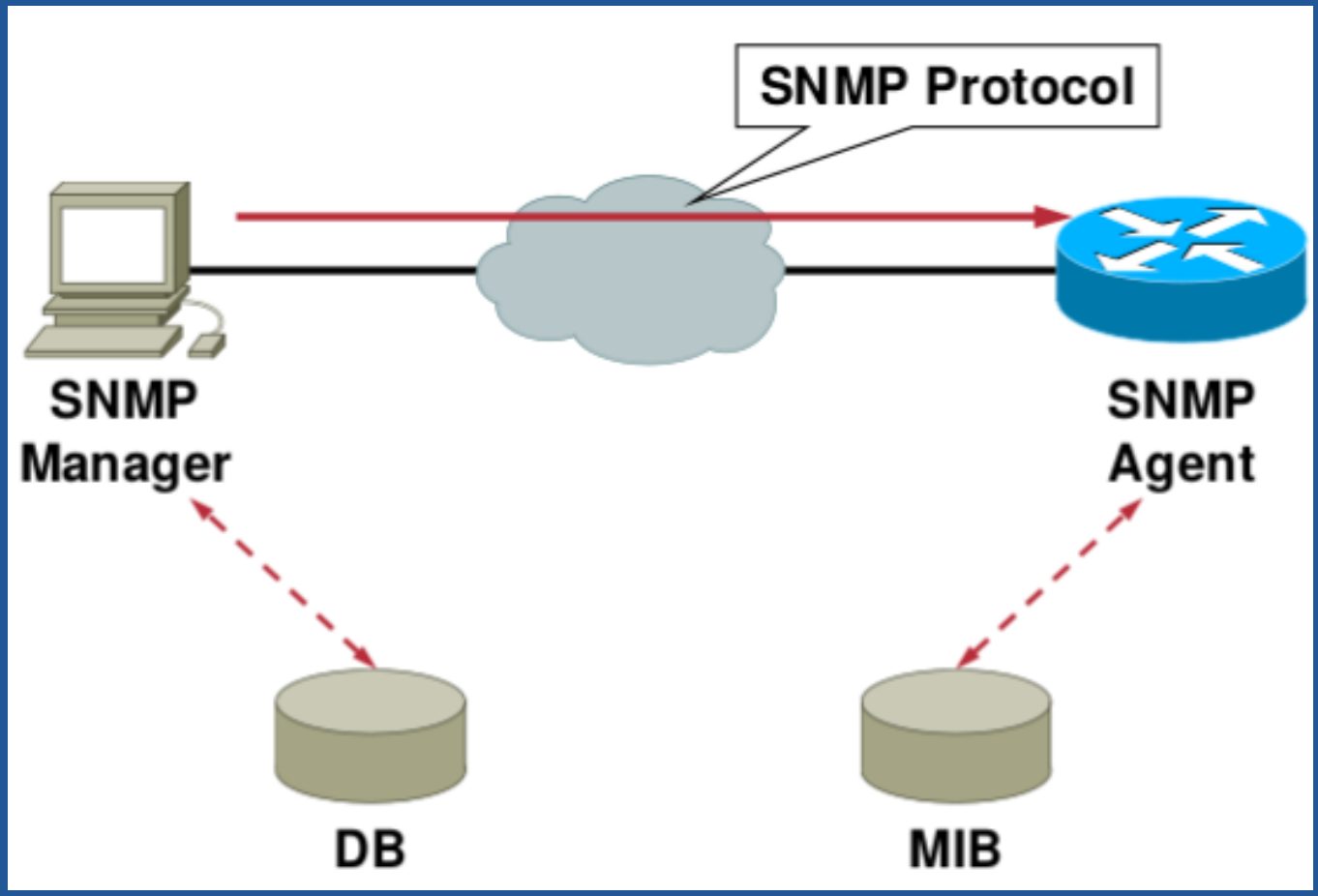
* Imagem: *Trafego IX.br (fonte: https://ix.br/agregado/)*

SNMP - Simple Network Management Protocol

SNMP

- Padrão de monitoramento de dispositivos de redes (rfc1157)
- Permite monitoramento de CPU, uso de memoria, disco, interfaces e contadores
- Arquitetura cliente-servidor
- Presente na maioria dos equipamentos e possibilidade de instalação em diversos sistemas
- Protocolo UPD, porta 161

Arquitetura de monitoramento via SNMP



* Imagem: *Arquitetura SNMP*

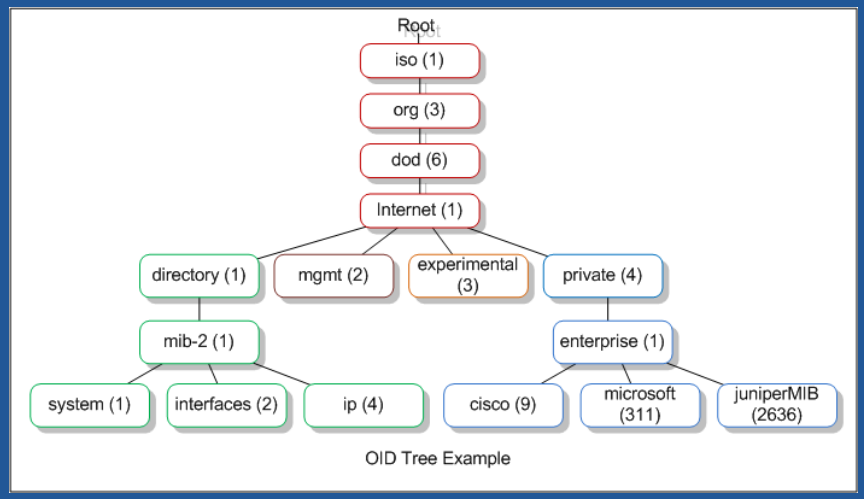
- Estação de Gerenciamento (Manager)
  - Agente de uma aplicação de gerencia
  - Inclui uma interface de operador, permitindo que um usuario/ferramenta autorizado possa gerenciar a rede
- Estação Agente
  - Está localizado dentro do dispositivo monitorado
  - Responde a requisições de informações e ações
  - Pode enviar notificações de falha ao gerenciador, i.e. uma mensagem *trap*
  - Troca informações usando protocolo SNMP

Protocolo de comunicação entre Gerentes e Agentes

- Possui três funcionalidades principais:
  - **GET**: Permite ao gerente (estação) recuperar valores de objetos dos agentes
  - **SET**: permite ao gerente configurar valores de objetos nos agentes
  - **NOTIFY**: Permite que agentes notifiquem o gerente a ocorrência de eventos significativos

MIB - Management Information Base

- Coleção de objetos a serem monitorados
- Cada objeto é um recurso e possui um ID associado (OID ou Object ID)



* Imagem: *Árvore de OID's*

Versões do SNMP

Versões do SNMP

- **SNMPv1**
  - Centralizado (pouca escalabilidade)
  - Não permite transferência de porções maiores de dados
- **SNMPv2**
  - Permite monitoramento descentralizado
  - Permite transferência de maiores porções de dados
  - Maior deficiência é a falta de segurança efetiva

Versões do SNMP

- **SNMPv3**
  - Autenticação
  - Autorização de usuários para monitorar e ler informações
  - Privacidade
  - Criptografia

Versões do SNMP

- Limitado a certos recursos disponibilizados pela implementação do fabricante
  - Estrutura rígida
  - Dependente de fabricante
- Necessita de rotinas internas de agregação de informação no plano de controle

Análises de trafego através de fluxos (Flow)

Fluxos

- Coleta de amostras (sample) de pacotes na rede
- Diversos protocolos
  - Netflow, Sflow, IPFIX, Netstream
- Difícil detectar anomalias de baixo nível
  - Amostragem, plano de controle, não tem informações do equipamento

Telemetria

Mudança na escala da rede fizeram com que modelos tradicionais, como SNMP, não performem e nem forneçam os dados necessários para verificar a saúde da rede

Telemetria

- Permite o sensoriamento através de uma interface mais universal e granular
  - Eventos interfaces, *buffer*, etc.
  - Adoção de modelo *PUSH*
- Diversas propostas
  - In-band Network Telemetry (INT)
  - Junos Telemetry Interface (JTI)
  - Cisco Model-Driven Telemetry (Streaming Telemetry)

Time-Series DataBase (TSDB)

Bancos de dados de series temporais

Time-Series DataBase (TSDB)

- **O que são? Para que servem?**
  - Evitar consumo desnecessário de espaço em disco
  - Formas eficientes de recuperação e inserção dos dados relacionados as métricas monitoradas
  - Desenvolvidos para armazenar métricas por longo períodos de tempo

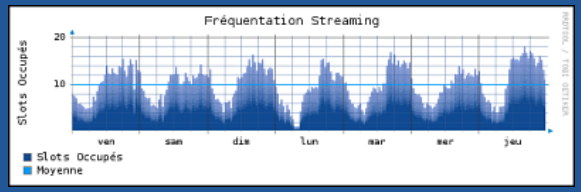
Time-Series DataBase (TSDB)

- Embora muitos TSDBs armazenamento eficiente das métricas, nem todos eles são voltados para inserções de dados continuas ou mesmo consultas que relacionem diversas métricas ou condições
- Um bom TSDB, além de ser eficiente na manipulação das métricas armazenadas e recuperadas do disco, deve permitir consultas customizáveis
- Na escolha de uma ferramenta de monitoramento de métricas temporais é necessário considerar o ecossistema da ferramenta escolhida:
  - Coletores, encaminhadores (proxies), monitoradores, visualizadores (front-end) e ferramenta de armazenamento (back-end)

Time-Series DataBase (TSDB)

RRDTool

- Um dos mais conhecidos e largamente utilizados
- Armazenamento de dados de maneira compacta, baixo uso de espaço em disco
- Dados são mantidos em forma circular: ao inserir novos dados, dados mais antigos são removidos



Time-Series DataBase (TSDB)

Graphite

- Dividido em 3 componentes: carbon (processador de métricas), whisper (biblioteca de TSDB) e web (visualização)
- Whisper: base de dados de tamanho fixo, provendo confiabilidade e rápido armazenamento de dados numéricos

Time-Series DataBase (TSDB)

InfluxDB

- Data store de alta performance
- NoSQL
- Data ingestion, compressão e consulta em tempo real sobre um mesmo dado e ao mesmo tempo

Time-Series DataBase (TSDB)

OpenTSDB

- Distribuído, escalável e desenhado para coletar, armazenar e servir bilhões de dados sem afetar a precisão
- Arquitetura de alta disponibilidade

Time-Series DataBase (TSDB)

TimescaleDB

- Implementado como extensão do PostgreSQL, suportando as mesmas operações e queires SQL
- Confiabilidade, segurança, conectividade e demais atributos já conhecidos
- Faz uso de hypertables, particionamento, virtual views e outras estrategias

TIMESCALE

Time-Series DataBase (TSDB)

Prometheus

- Desevolvido para gravação de dados em tempo real usando modelo pull via HTTP
- Queries flexíveis e alertas em tempo real
- possui linguagem própria para consulta de dados
- dados são gravados como métricas identificadas por nome

Prometheus

Prometheus

an open-source systems monitoring and alerting toolkit

Principais funcionalidades

- Modelo multidimensional de dados: séries de dados identificadas métricas e pares de chave/valor
- Linguagem de consulta flexível (**PromQL**)
  - Suporte a operadores lógicos, aritméticos e agregadores (sum, min, avg, etc)
- Não depende de armazenamento distribuído; nós de um único servidor são autônomos
- As coletas de séries temporais são realizadas via HTTP Pull (**exporter**)

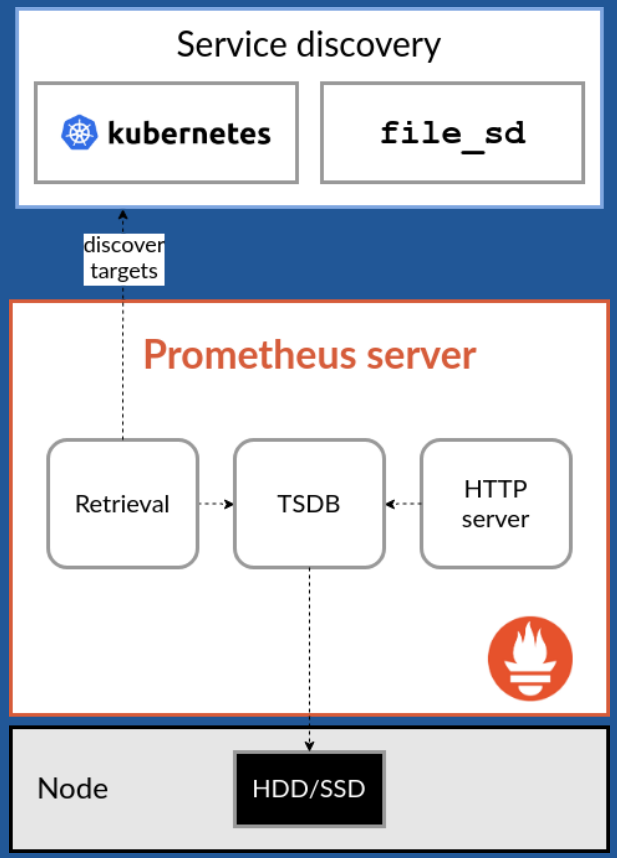
Principais funcionalidades

- O envio (**push**) de séries temporais pode ser feito via gateway intermediário (**push gateway**)
- Alvos (**targets**) são descobertos via service discovery ou configuração estática
- Suporta múltiplos modos de apresentação de dados (**graphing and dashboarding**)

Componentes

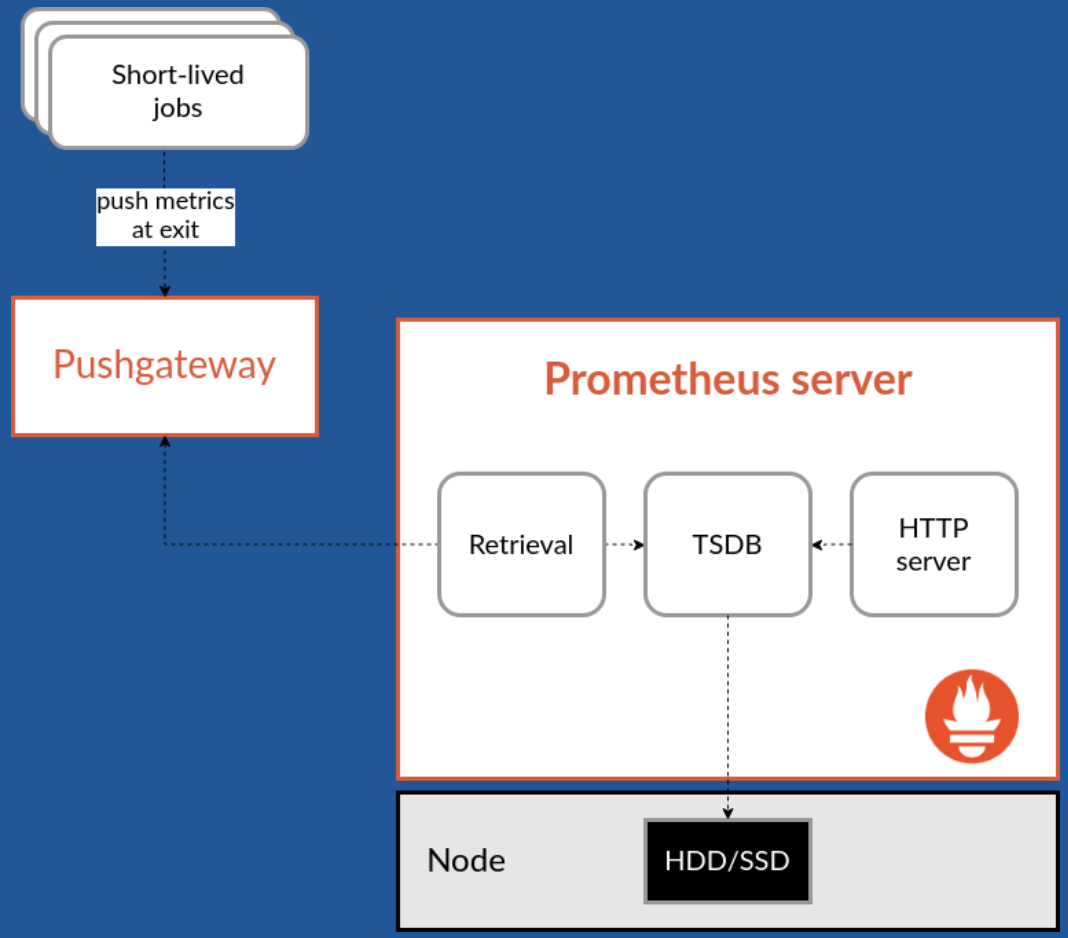
- Servidor de coleta (**scrapes**) e armazena séries de dados temporais (**Prometheus server**)
- Bibliotecas de cliente (**client libaries**) para programação
- **push gateway** para suportar jobs de curta duração
- Exportadores (**exporters**) para diversos serviços: SNMP, StatsD, Graphite, etc
- O **alertmanager** para disparar alertas
- Outras ferramentas de suporte

Prometheus Server



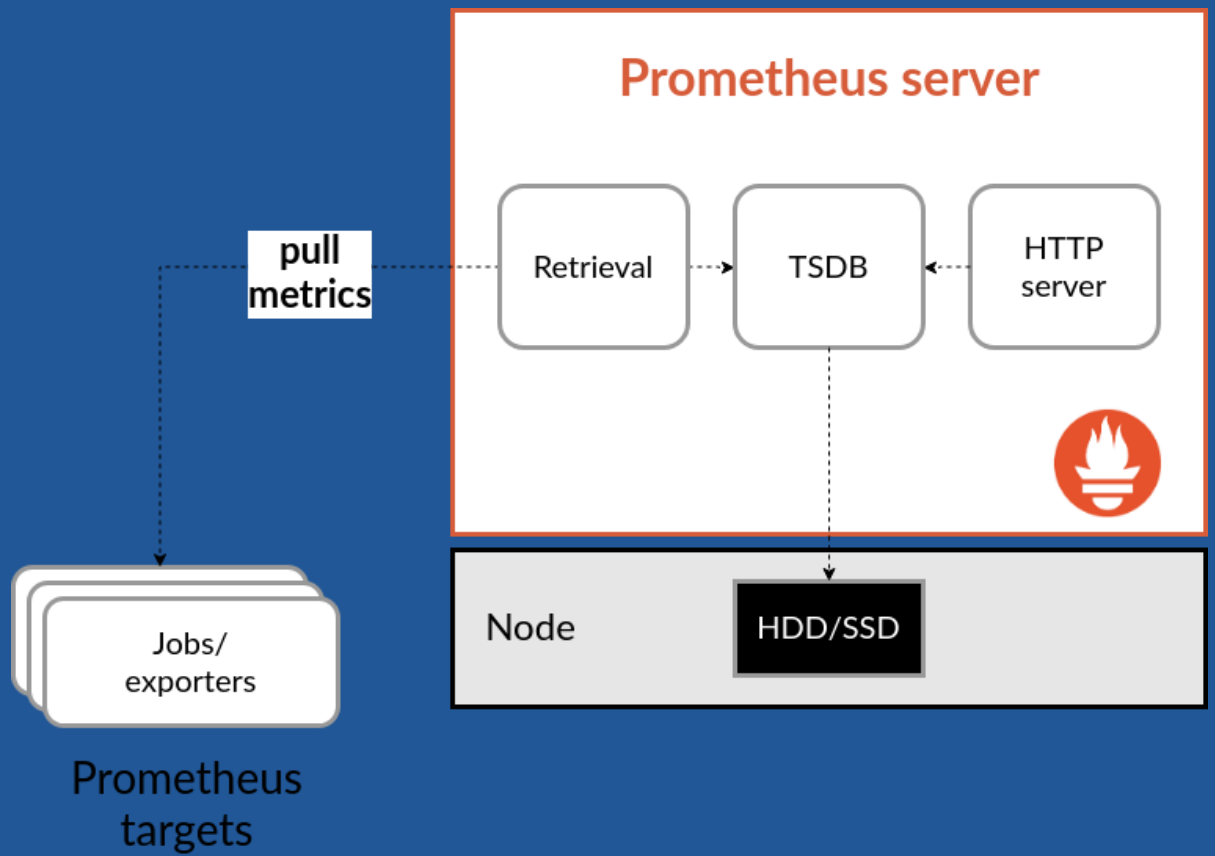
* Imagem: *Servidor Prometheus*

Push Gateway



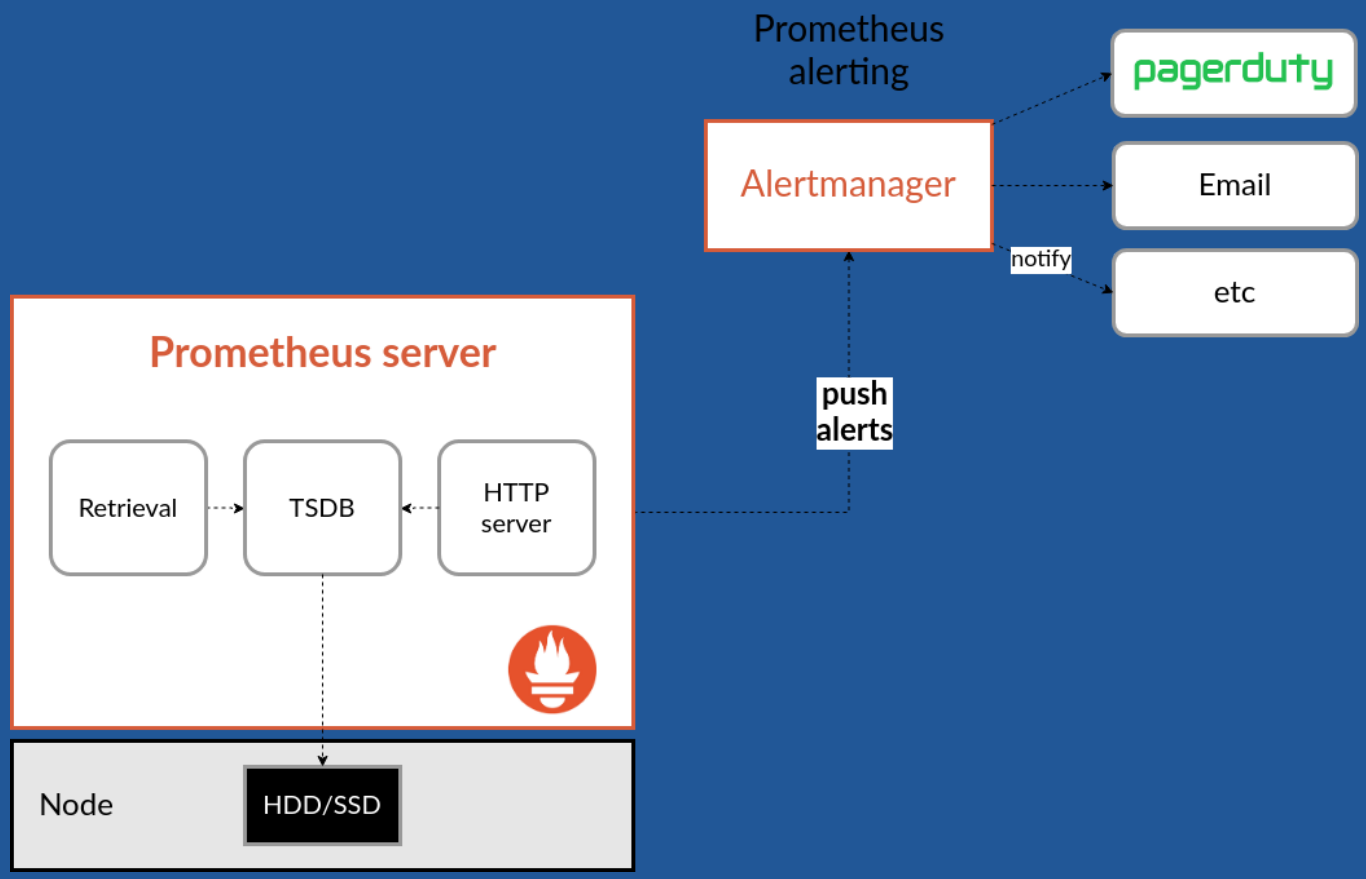
* Imagem: *Push Gateway*

Exporters



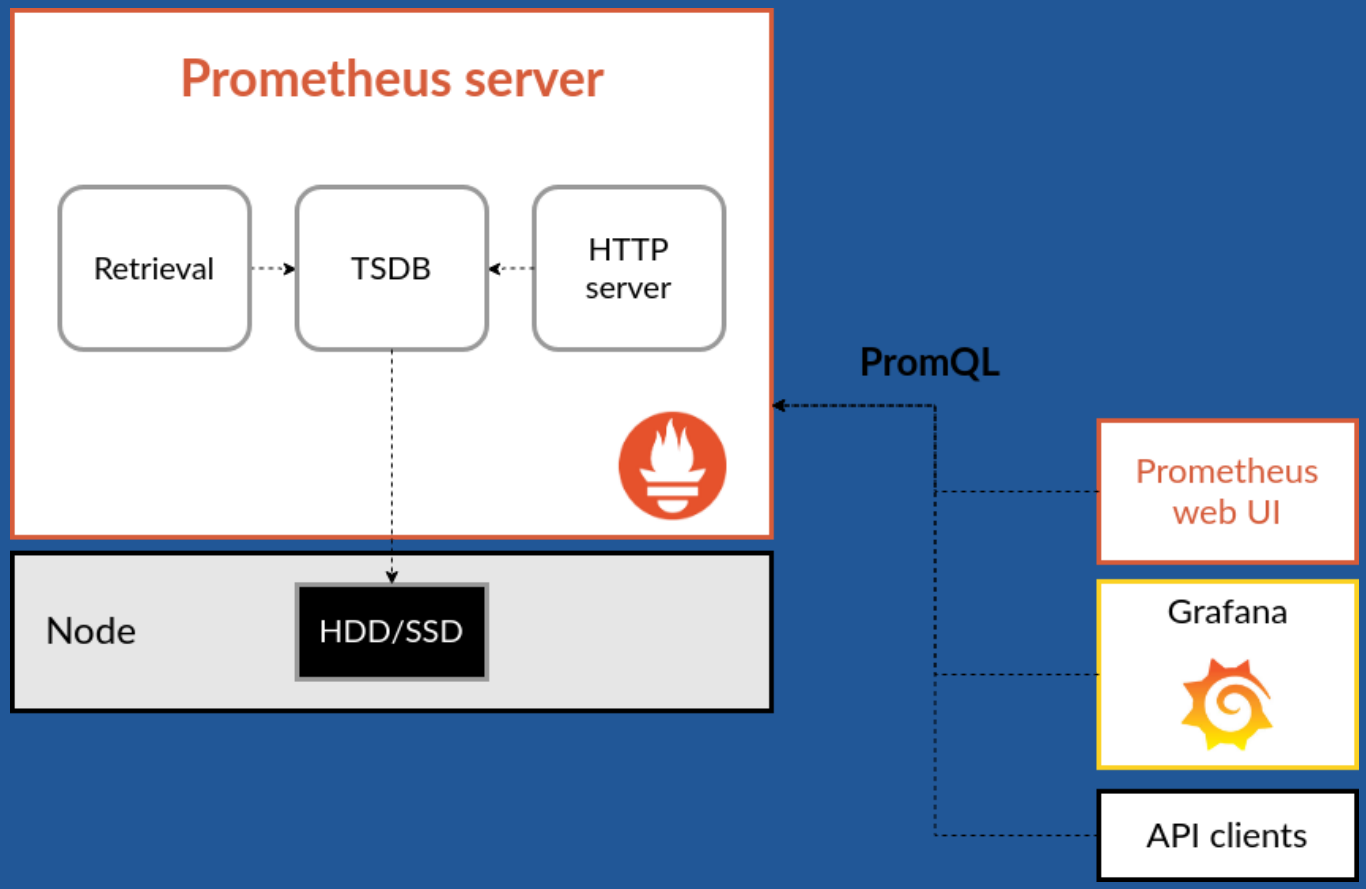
* Imagem: *Prometheus Targets and Exporters*

Alertmanager



* Imagem: *Prometheus Alerting*

Data Visualization



* Imagem: *Data Visualization*

Grafana

The open observability platform

Grafana

- Plataforma para monitoramento e observabilidade (monitoring e observability)
- Visualização e suporte para diversas fontes de dados (data sources), incluindo **Prometheus**
- Realização de buscas, visualização e emissão de alertas
- Criação de múltiplos dashboards e possui um conjunto de templates disponíveis
- Criação de gráficos com combinações de múltiplos datasets (mixed data sources)

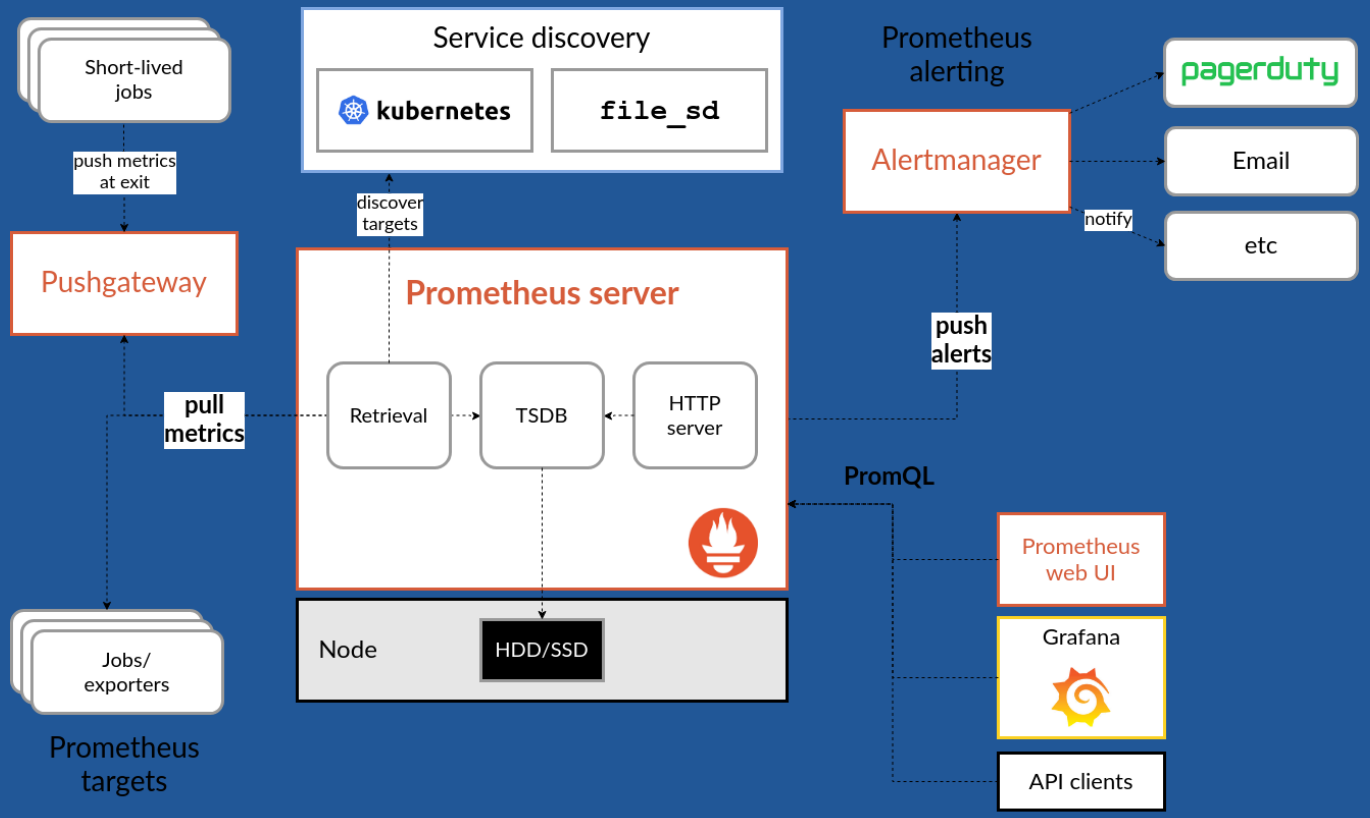
Datasources

- Suporta diversos tipos de data sources
  - Time series databases: Prometheus, Graphite, OpenTSDB, InfluxDB
  - Logging and Documents databases: Elastic Search, Loki
  - SQL databases: MySQL, PostgreSQL, Microsoft SQL Server
  - Nuvem: Azure, GCE/GKE, AWS
  - Entre outros plugins desenvolvidos pela comunidade

Dashboard

* Imagem: *Exemplo de Dashboard*

Arquitetura da solução



* Imagem: *Arquitetura da Solução de Monitoramento*

Referências

- The USE Method: http://www.brendangregg.com/usemethod.html
- Monitoring Distributed Systems: https://landing.google.com/sre/sre-book/chapters/monitoring-distributed-systems/
- The RED Method: key metrics for microservices architecture: https://www.weave.works/blog/the-red-method-key-metrics-for-microservices-architecture/
- BADER, Andreas. Comparison of Time Series Databases. 2016. Tese de Doutorado. Diploma Thesis, Institute of Parallel and Distributed Systems, University of Stuttgart.
- PETRE, Ionut et al. A Time-Series Database Analysis Based on a Multi-attribute Maturity Model. Studies in Informatics and Control, v. 28, n. 2, p. 177-188, 2019.
- BADER, Andreas; KOPP, Oliver; FALKENTHAL, Michael. Survey and Comparison of Open Source Time Series Databases. In: BTW (Workshops). 2017. p. 249-268.
- Referencias Prometheus + Grafana + Gauge: https://wiki.openvz.org/SNMPD_in_container

Referências

- SNMP Exporter: https://labs.consol.de/omd/howtos/prometheus_snmp_exporter/
- snmp_exporter：SNMP Exporter for Prometheus: https://www.diycode.cc/projects/prometheus/snmp_exporter
- Prometheus: Prometheus monitoring switch (snmp): https://programmer.group/prometheus-prometheus-monitoring-switch-snmp.html
- Prometheus: snmp_exporter and OpenBSD: https://yetiops.net/posts/openbsd-snmp-exporter/
- Streaming Telemetry: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming-telemetry
- In-band Network Telemetry (INT): https://p4.org/assets/INT-current-spec.pdf
- Junos Telemetry Interface User Guide: https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/junos-telemetry-interface/junos-telemetry-interface.pdf

WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

Monitoramento de ativos de rede com ferramentas de código aberto

Ibirisol Fontes e Jundai Abdon

PoP-BA Ponto de Presença da RNP na Bahia
RNP 30 anos
MINISTÉRIO DA DEFESA
MINISTÉRIO DA CIDADANIA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
PÁTRIA AMADA BRASIL GOVERNO FEDERAL