ZABBIX

MONITORAMENTO DE ATIVOS EM PROVEDORES UTILIZANDO O ZABBIX COMO SOLUÇÃO

QUEM SOU EU?

ZABBIX

Victor Breda Credidio

- Formado em Ciência da computação;
- Pós-graduado em Segurança da informação;
- LPIC-01/Comptia Linux+
- Zabbix Certified Trainer
- Engenheiro de Suporte Global

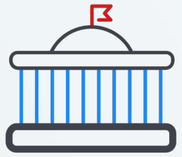
/in/victor-bc

SOBRE O ZABBIX

ZABBIX

O ZABBIX É UMA SOLUÇÃO OPEN SOURCE, GRATUITA, E DE CLASSE EMPRESARIAL, QUE FORNECE MONITORAMENTO EM VÁRIOS NÍVEIS

É UTILIZADO MUNDO A FORA POR EMPRESAS DE VÁRIOS SEGUIMENTOS COMO TELECOMUNICAÇÕES, FINANCEIRO, EDUCACIONAL, VAREJO, E COMPANHIAS DE VÍNCULO HOSPITALAR



SOBRE O ZABBIX

O SOFTWARE SURGIU EM 2001 E TEVE SUA VERSÃO 1.0 LANÇADA EM 23 DE MARÇO DE 2004

NO ANO SEGUINTE FOI ESTABELECIDA A NOSSA MATRIZ EM RIGA, NA LETÔNIA

HOJE POSSUI ESCRITÓRIOS AO REDOR DO MUNDO (SEM CONTAR COM NOSSOS PARCEIROS OFICIAIS):

- **Europa**
- **Japão**
- **EUA**
- **América Latina – POA**
- **América Latina – Cid. do México**

O QUE É MONITORAMENTO?

ZABBIX

DEFINIÇÃO DE MONITORAMENTO

"Um contínuo processo de coleta e análise de métricas sobre um programa, projeto, ou negócio, e comparação entre resultados atuais e resultados planejados, de forma a julgar o andamento de sua implementação."

Fonte: *International Labor Organization*

Conta com ferramentas e tecnologias para:

- Coletar
- Apresentar
- Analisar
- Auxiliar na tomada da ações

POR QUÊ MONITORAR?

ZABBIX

- **CONTROLE**
- **VISIBILIDADE**
- **ALCANÇAR OBJETIVOS/METAS COM MENOR NÚMERO DE DESVIOS**

Negócio

- Planejamento de capacidade
- Redução de custo
- Acompanhar KPIs
- Monitoramento a nível de serviço
- Prover MaaS

METAS

Infraestrutura

- Controle do ambiente de TI
- Detectar gargalos na infraestrutura
- Solução de NOC centralizada
- Remediação de problemas pró-ativo
- Lógica de alerta flexível

COMO FUNCIONA?

ZABBIX

ZABBIX SERVER (BACKEND)

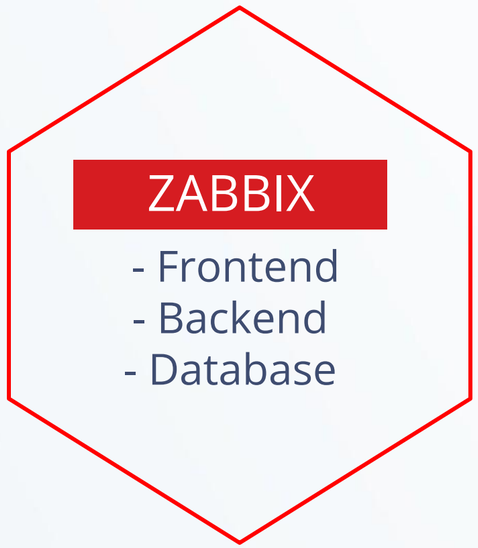
- Processo central responsável pela coleta e análise de dados

DATABASE

- Armazenamento de dados e configurações

FRONTEND

- Frontend em PHP para gerência das configurações e visualização de dados



Visualização

Notificações

COMO FUNCIONA?

ZABBIX

ZABBIX SERVER (BACKEND)

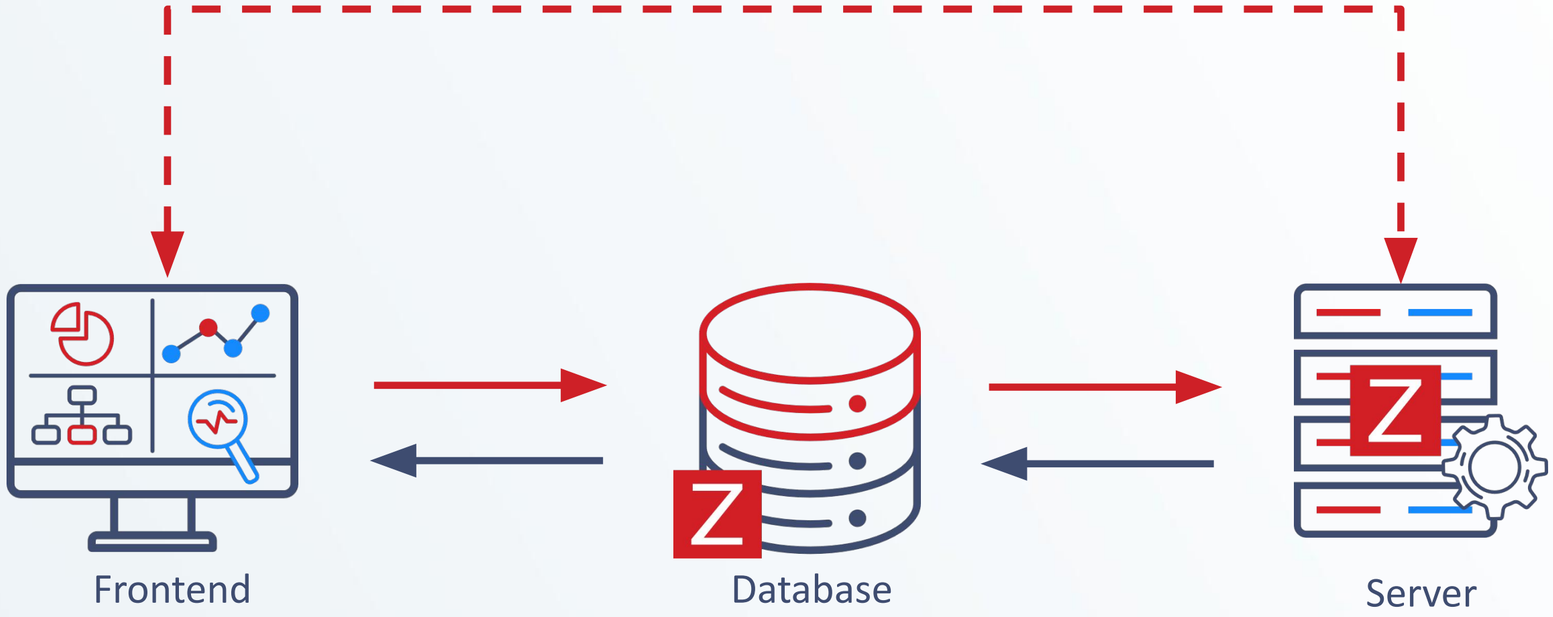
- Processo central responsável pela coleta e análise de dados

DATABASE

- Armazenamento de dados e configurações

FRONTEND

- Frontend em PHP para gerência das configurações e visualização de dados



COMO FUNCIONA?

ZABBIX

ZABBIX SERVER (BACKEND)

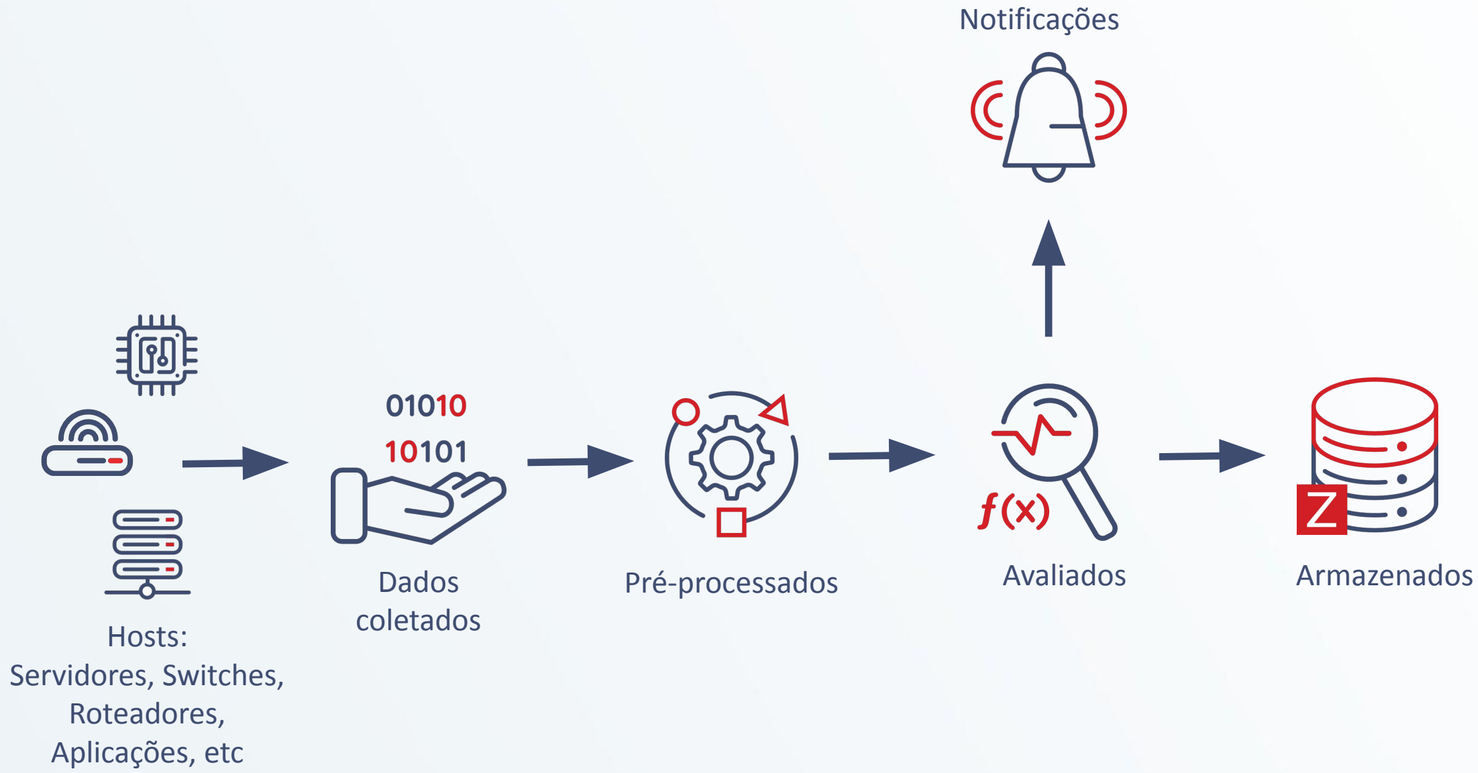
- Processo central responsável pela coleta e análise de dados

DATABASE

- Armazenamento de dados e configurações

FRONTEND

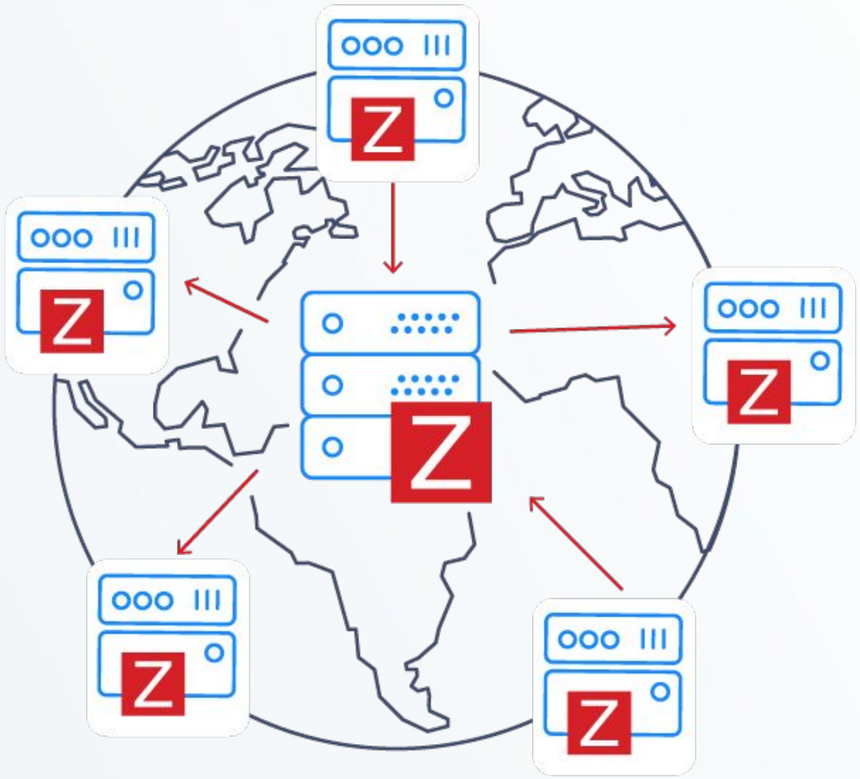
- Frontend em PHP para gerência das configurações e visualização de dados



MONITORAMENTO DISTRIBUÍDO

Zabbix proxies em locais remotos para redundância e fácil configuração

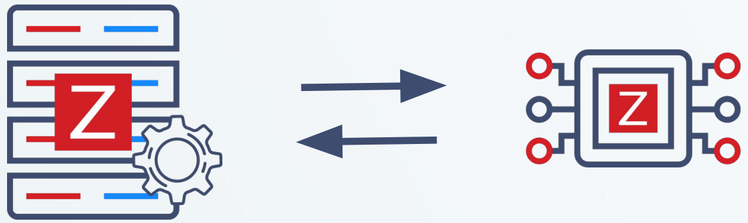
- Compressão de dados
- Monitoramento atrás de um firewall, DMZ
- Coleta de dados em caso de problema de rede
- Execução de scripts em hosts monitorados
- Controle de todos os proxies através de uma página



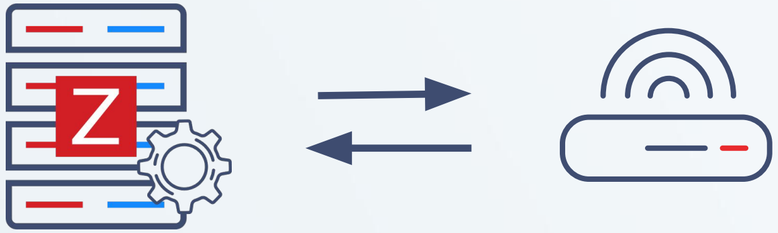
COLETA DOS DADOS

ZABBIX

- **ATRAVÉS DE UM AGENTE**



- **SEM AGENTE (AGENTLESS)**

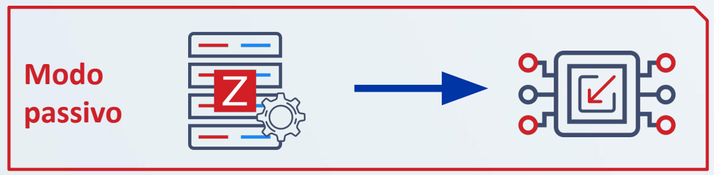


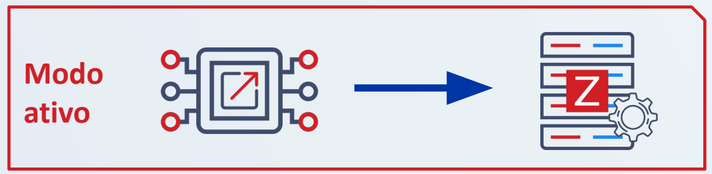
COLETA DOS DADOS

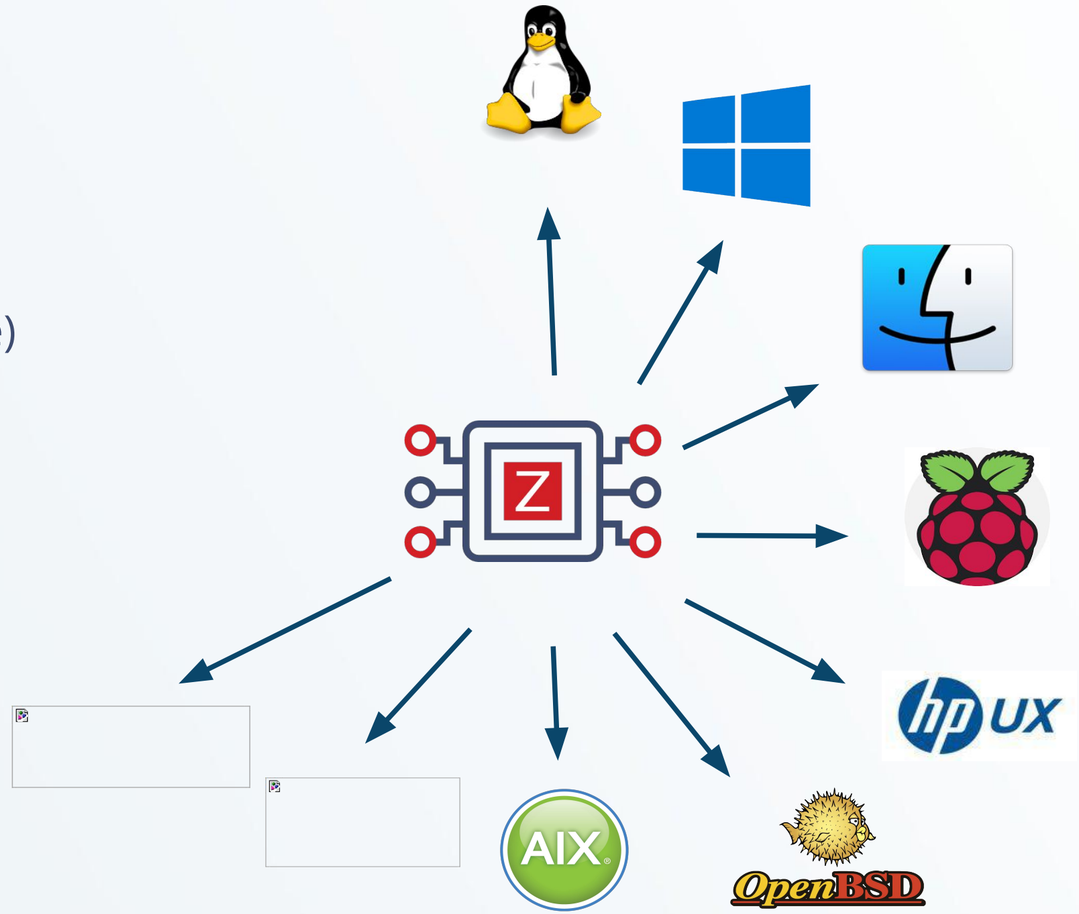
ZABBIX

Coleta com agente

- Pode rodar em várias plataformas
- Coleta dados de um dispositivo ou aplicação
- Baixo footprint de memória e uso de recursos
- Pode funcionar nos modos ativo e passivo (simultaneamente)
- Suporta comunicação encriptada e forma nativa







COLETA DOS DADOS

ZABBIX

Coleta sem agente

- Monitoramento é realizado diretamente pelo Zabbix server ou Proxy
- Coleta baseada em protocolos de redes:
  - Ping e verificação de portas
  - SNMP (v1, v2, v3)
  - HTTP
  - IPMI
  - SSH
  - Monitoramento de aplicações JAVA
  - Banco de dados via ODBC
  - Scripts customizados
  - Nem o céu é o limite...

COLETA DOS DADOS

ZABBIX

Coleta sem agente

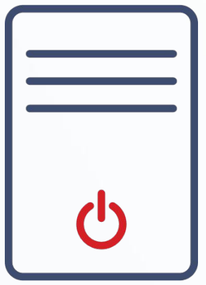
- Monitoramento é realizado diretamente pelo Zabbix server ou Proxy
- Coleta baseada em protocolos de redes:
  - Ping e verificação de portas
  - **SNMP (v1, v2, v3)**
  - HTTP
  - IPMI
  - SSH
  - Monitoramento de aplicações JAVA
  - Banco de dados via ODBC
  - Scripts customizados
  - Nem o céu é o limite...

CONCEITOS BÁSICOS

ZABBIX

Hosts

Todo objeto ou alvo do qual queremos extrair métricas (Servidores, Switches, Roteadores, Aplicações, etc)



Item
É o que de fato indica as métricas que vão ser coletas (CPU, RAM, Uptime, Temperatura, etc)

Trigger
Responsável pela avaliação do valor da métrica coletada (Problema ou OK)

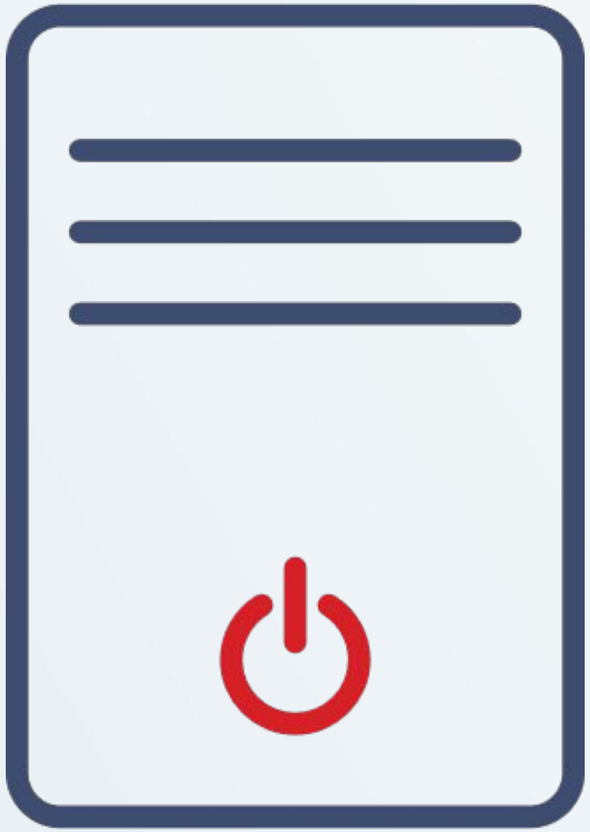
Template
Conjunto de entidades (Item, Trigger, Gráficos) que pode ser aplicado a múltiplos hosts

- **Action**

  Conjunto de condições que, caso sejam atendidas, executa um conjunto de operações automaticamente

HOSTS

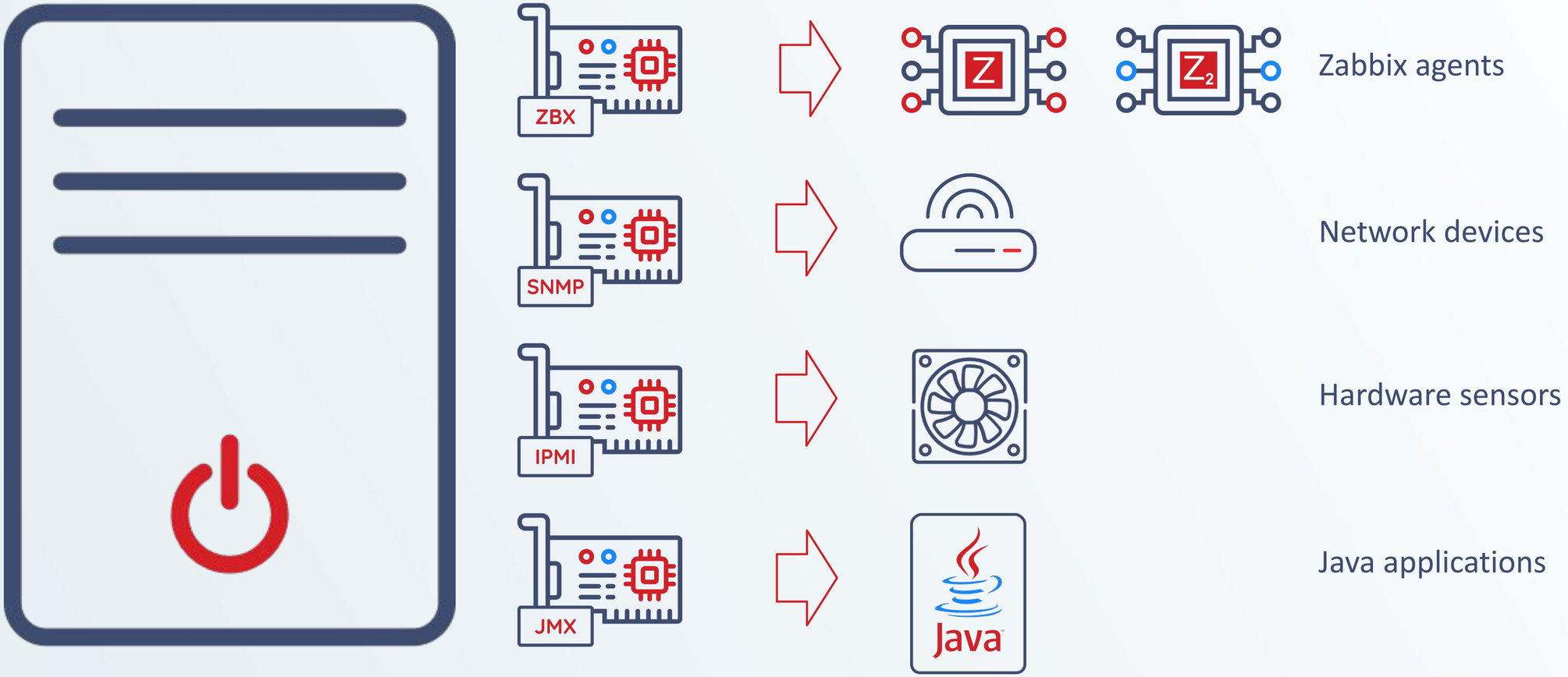
Todo objeto ou alvo do qual queremos extrair métricas (Servidores, Switches, Roteadores, Aplicações, etc)



- Items
- Triggers
- Gráficos
- Cenários Web
- Regras de descoberta de baixo nível (LLD)

INTERFACES DO HOST

Dentro do Zabbix, as informações são capturadas pelos Hosts a partir de interfaces



Zabbix agents

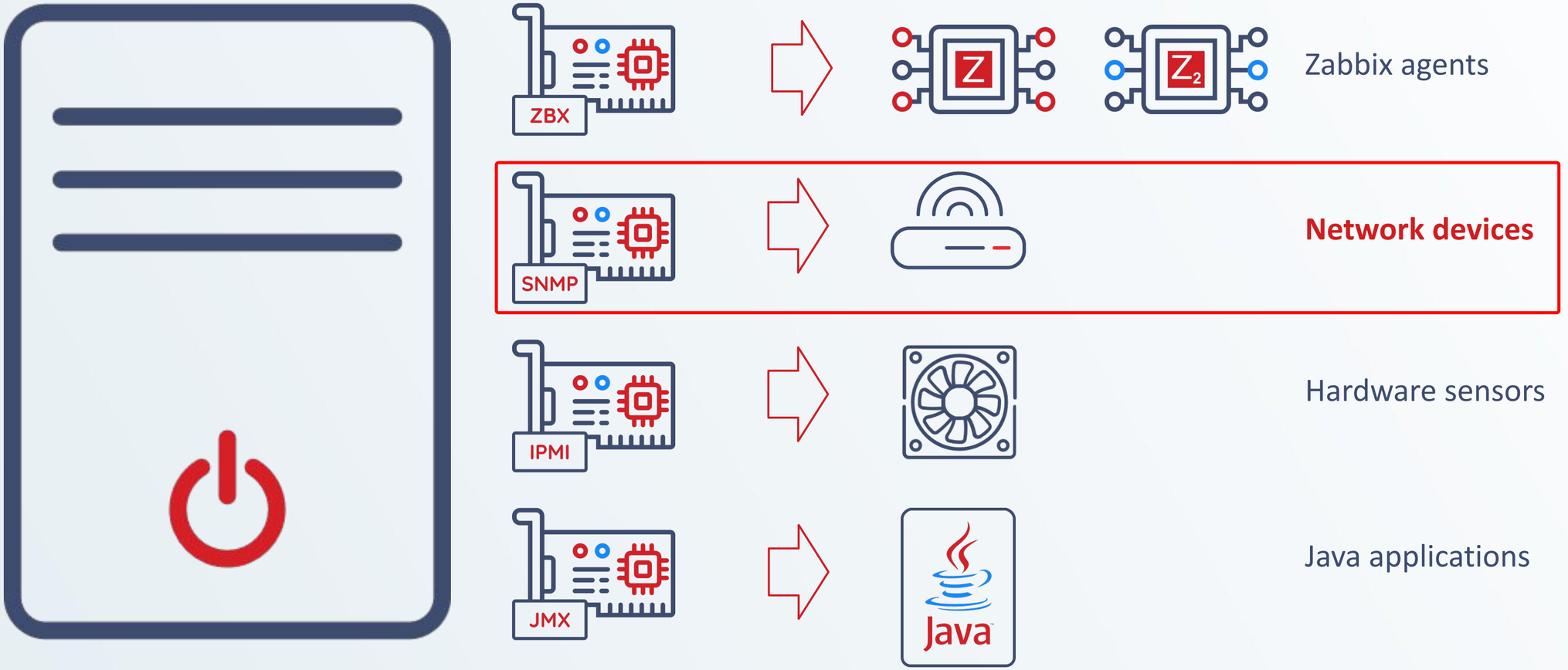
Network devices

Hardware sensors

Java applications

INTERFACES DO HOST

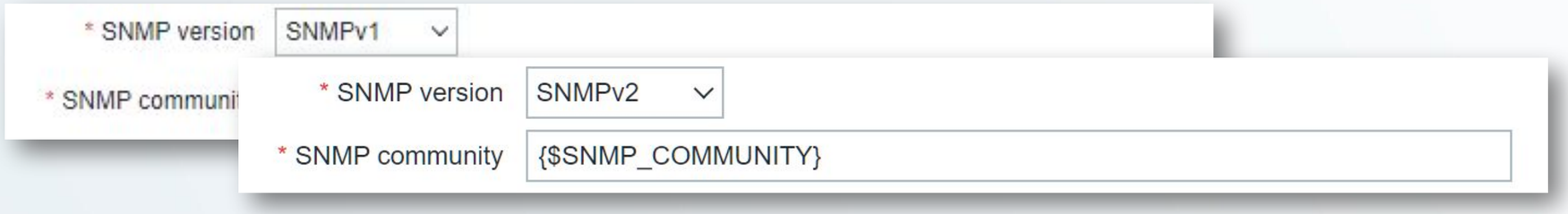
Dentro do Zabbix, as informações são capturadas pelos Hosts a partir de interfaces



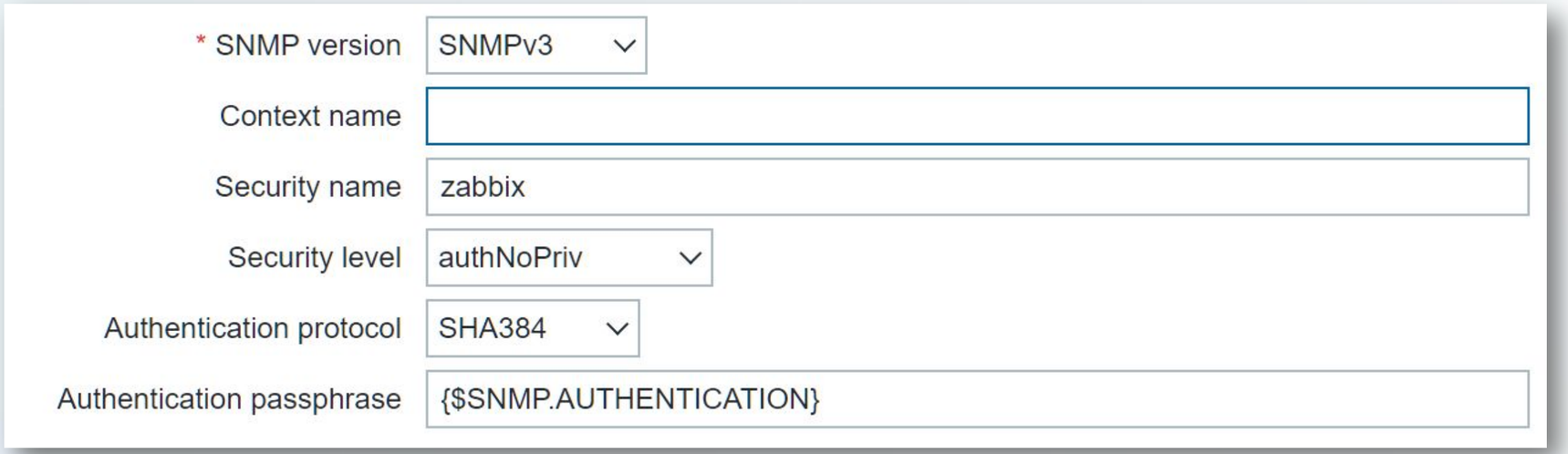
INTERFACES DO HOST

ZABBIX

SNMPv1 e v2 temos que passar o nome da comunidade SNMP utilizada



SNMPv3 oferece demais parâmetros de segurança



ITEMS

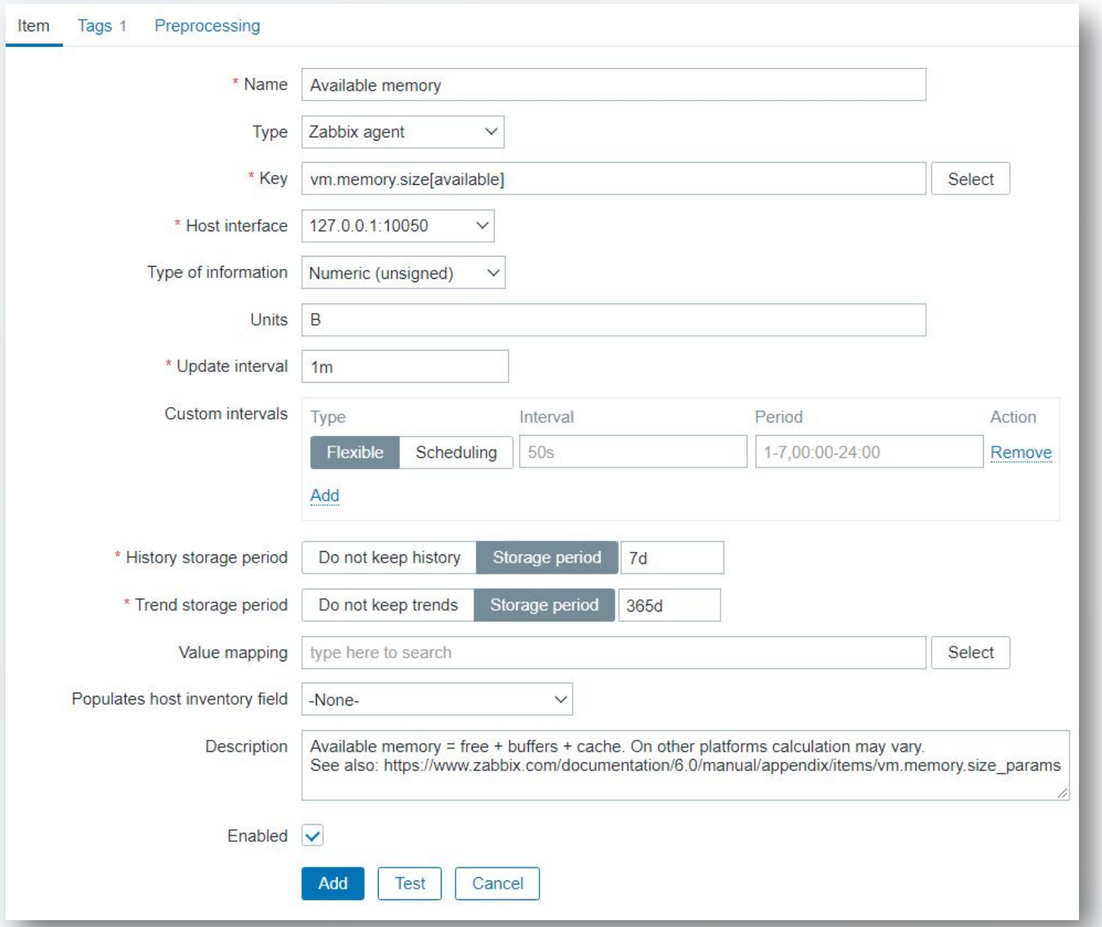
ZABBIX

Cada interface é utilizada para determinados tipos de items/métricas
O tipo do item determina como a métrica vai ser coletada:

- **Forma passiva (requisição):**
  - Zabbix agent
  - Simple check
  - SNMP agent
  - IPMI agent
  - JMX agent
  - HTTP agent
  - SSH agent
  - Telnet agent
  - Database monitor
  - External check
  - Script

- **Forma ativa (captura):**
  - Zabbix agent (active)
  - SNMP trap
  - Zabbix trapper
  - HTTP agent if "Enable trapping" is set

- **Meios internos:**
  - Zabbix internal
  - Calculated
  - Dependent item



ITEMS

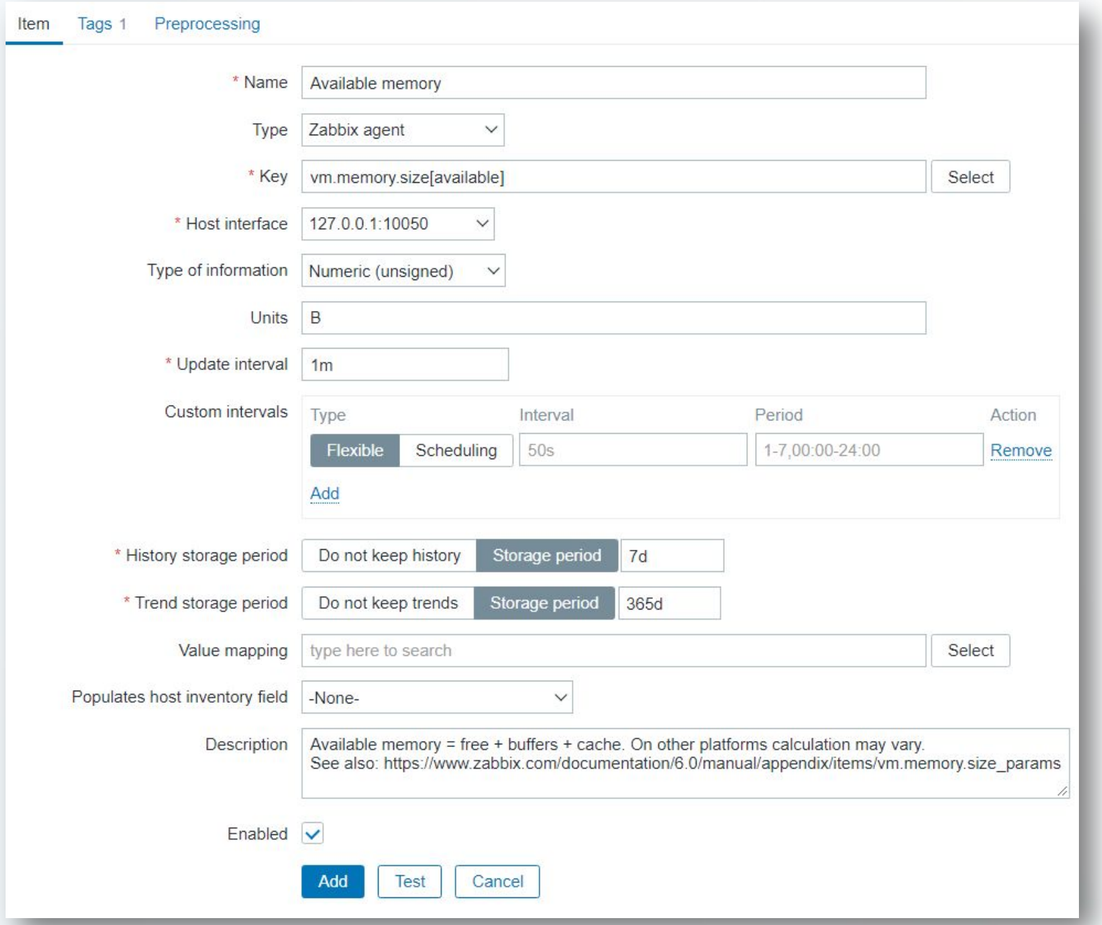
ZABBIX

Cada interface é utilizada para determinados tipos de items/métricas
O tipo do item determina como a métrica vai ser coletada:

- **Forma passiva (requisição):**
  - **Zabbix agent**
  - **SNMP agent**
  - **IPMI agent**
  - **JMX agent**
  - Simple check
  - HTTP agent
  - SSH agent
  - Telnet agent
  - Database monitor
  - External check
  - Script

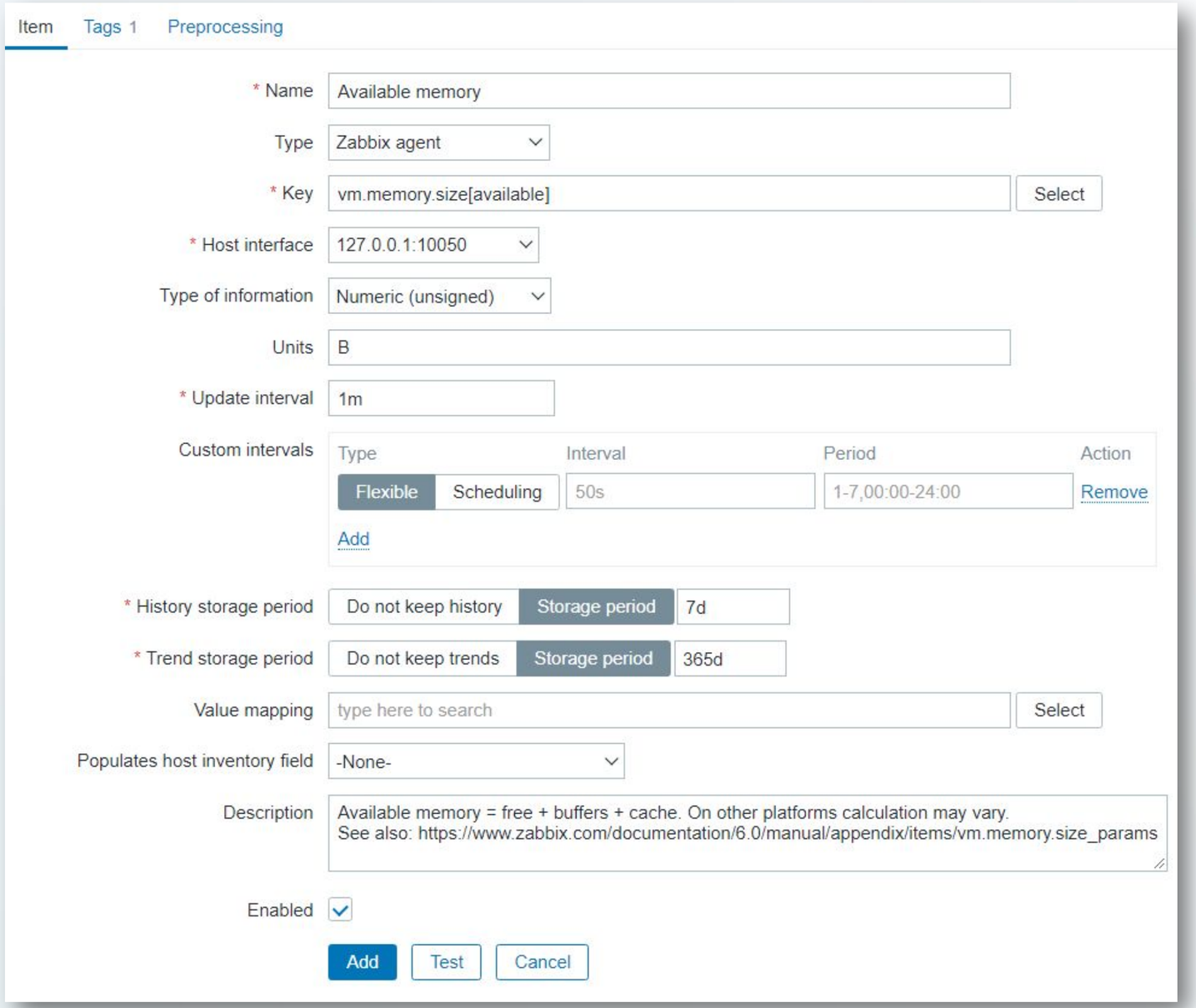
- **Forma ativa (captura):**
  - **Zabbix agent (active)**
  - **SNMP trap**
  - Zabbix trapper
  - HTTP agent if "Enable trapping" is set

- **Meios internos:**
  - Zabbix internal
  - Calculated
  - Dependent item



ITEMS

ZABBIX



TRIGGER

ZABBIX

Responsável pela avaliação do valor da métrica coletada

- São expressões lógicas que definem um limiar/threshold para os valores coletados
    - Exemplo:
      Se a média nos últimos 5 minutos da carga de CPU do meu servidor de produção for maior do que 2, então consideramos isso um problema

avg(/servidor de produção/system.cpu.load,5m)>2

- Caso essa expressão seja VERDADEIRA, a trigger assume o estado de PROBLEMA

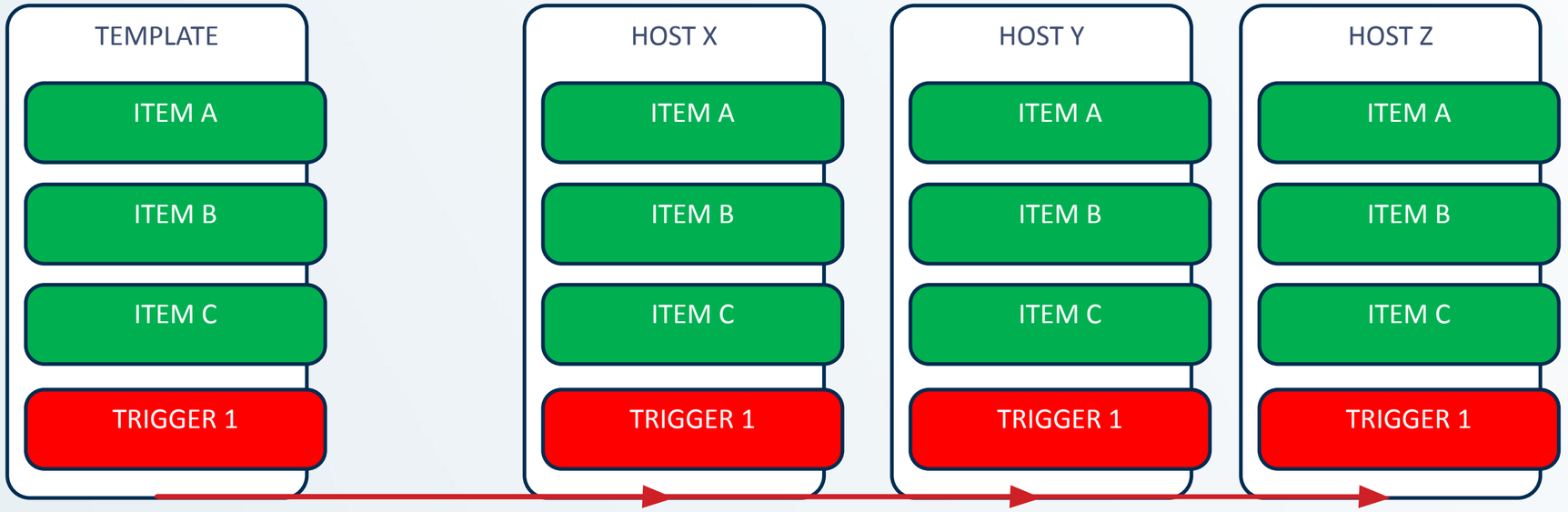
Trigger status	Description
OK	Trigger em estado normal (aceitável)
PROBLEM	Problema detectado pelo dado avaliado

TEMPLATE

ZABBIX

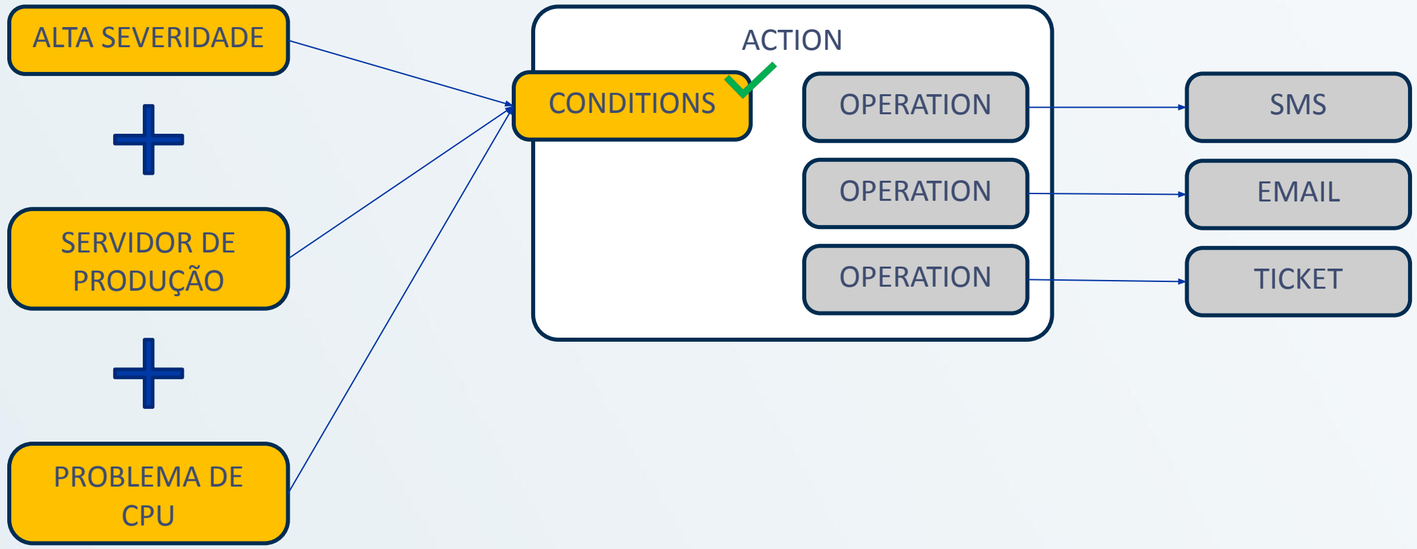
Conjunto de entidades que pode ser aplicado a múltiplos hosts

- Agilidade
- Simplicidade
- Facilidade de gerência de centenas/milhares de Hosts



ACTION

Conjunto de condições que, caso sejam atendidas, executa um conjunto de operações automaticamente



- Enviar um e-mail para suporte N1 imediatamente
  - Após 1 hora, para suporte N2
  - Após 2 horas, SMS para Admin
  - Após 3 horas, reinicia o servidor
  - Após 6 horas, reboot do DC

VISUALIZAÇÃO - DASHBOARDS

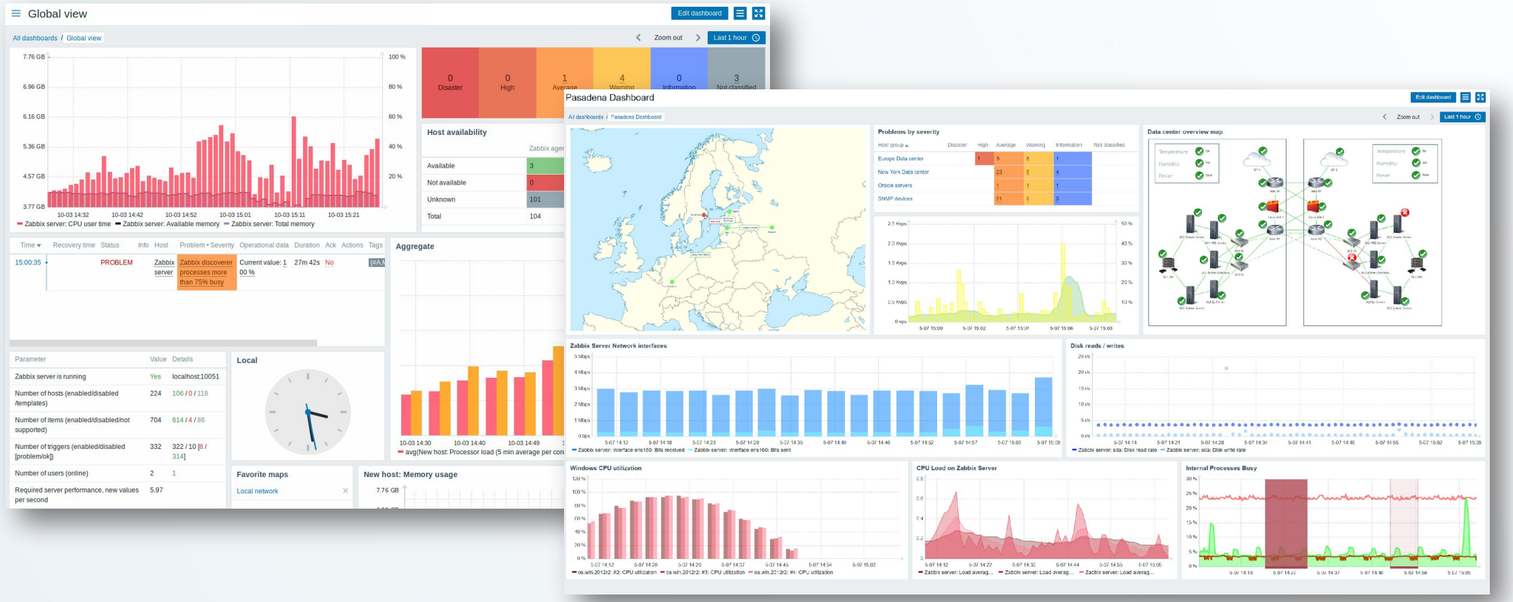
Através de Dashboards é possível visualizar um resumo de sua operação

Eles podem ter uma ou várias páginas, que podem ser rotacionadas em um Slide show de forma automática

Dashboards são baseados em widgets, pequenos painéis que trazem determinados tipos de informação

Exemplos de Widgets:

- Gráficos
- Mapas
- Valores isolados
- Resumo de problemas
- Relógio
- Entre outros...
- Personalizados



DASHBOARDS DE HOSTS

ZABBIX

- **DASHBOARDS DEDICADOS E ESPECÍFICOS PARA OS HOSTS**
- **SÃO HERDADOS DE TEMPLATES**
- **APENAS ALGUNS WIDGETS PODEM SER UTILIZADOS**

VISUALIZAÇÃO - DASHBOARDS

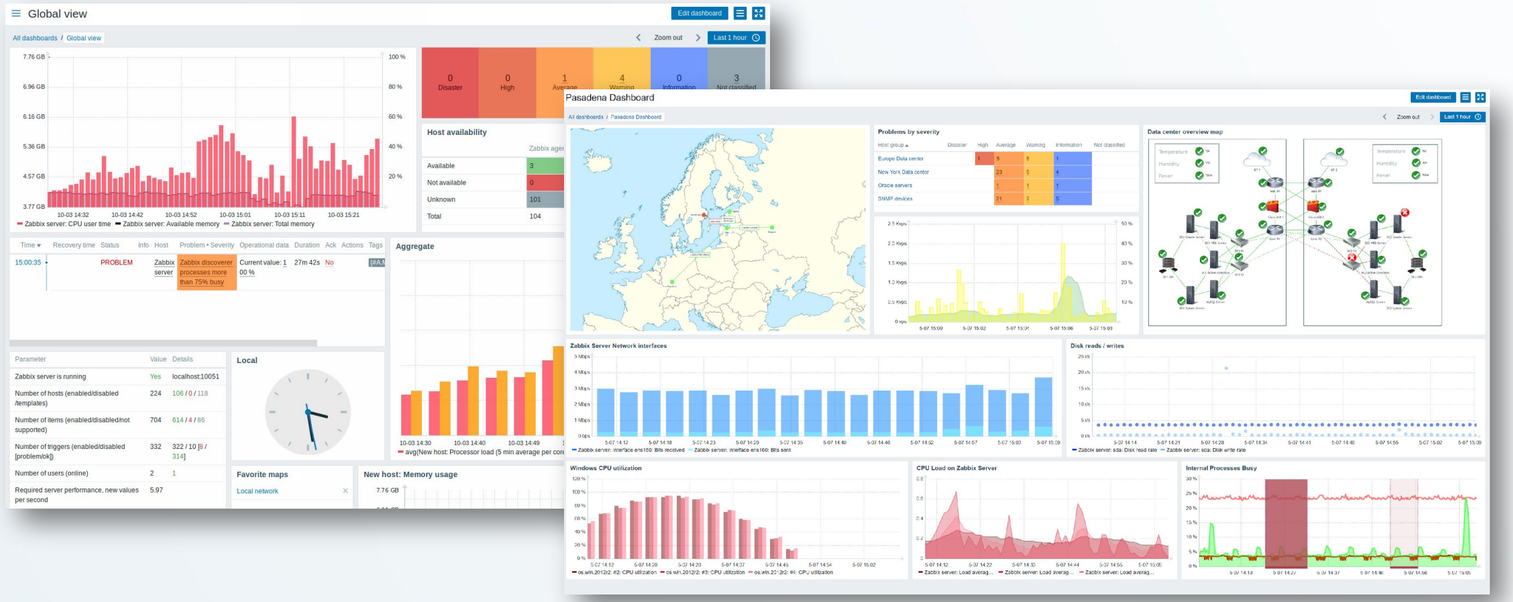
Através de Dashboards é possível visualizar um resumo de sua operação

Eles podem ter uma ou várias páginas, que podem ser rotacionadas em um Slide show de forma automática

Dashboards são baseados em widgets, pequenos painéis que trazem determinados tipos de informação

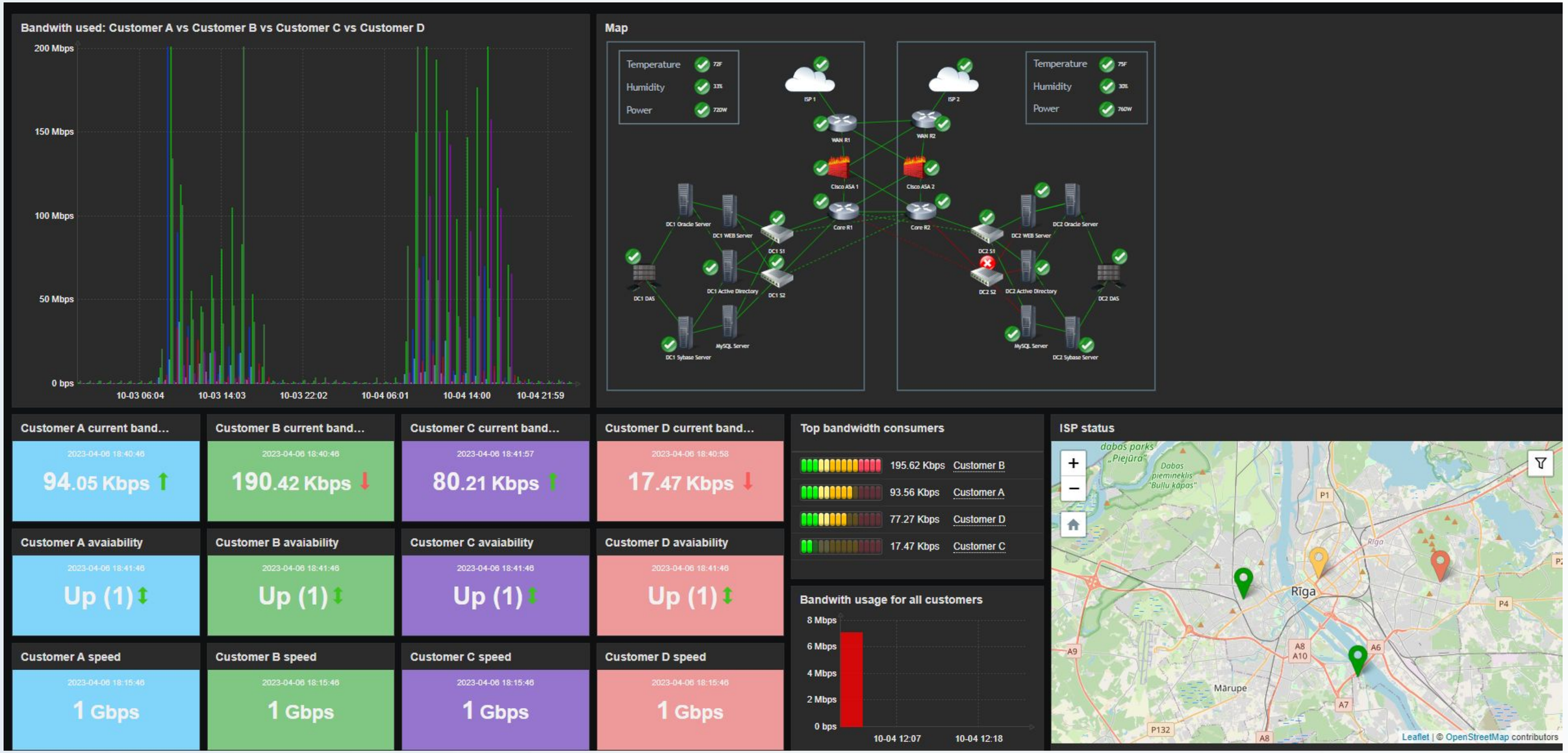
Exemplos de Widgets:

- Gráficos
- Mapas
- Valores isolados
- Resumo de problemas
- Relógio
- Entre outros...
- Personalizados



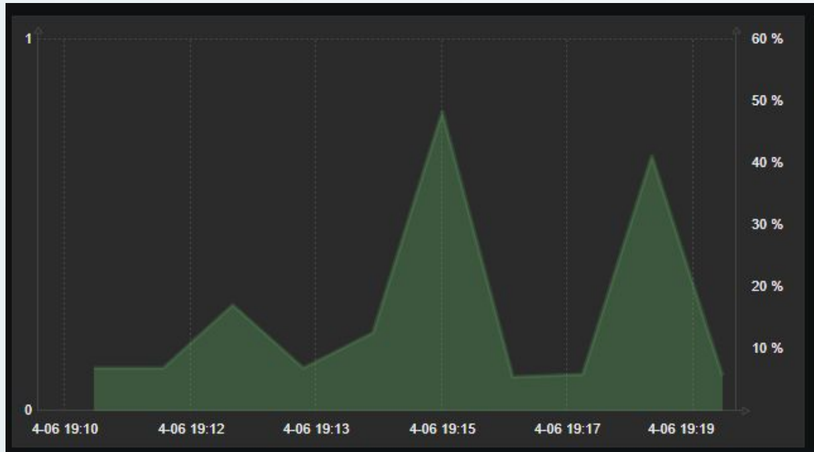
VISUALIZAÇÃO

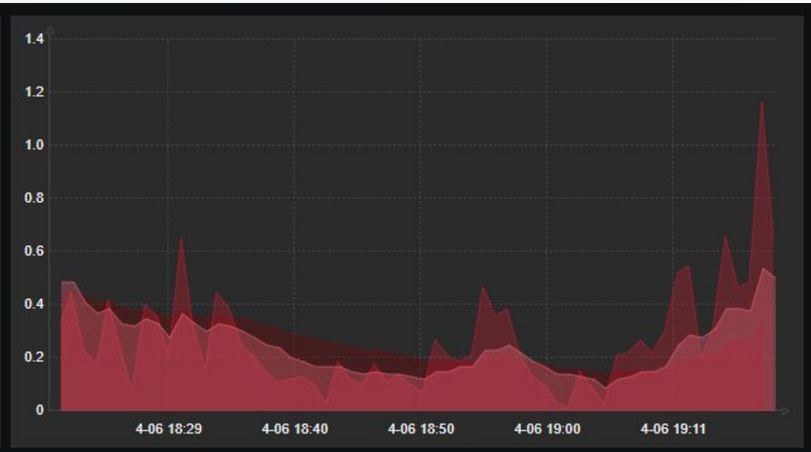
ZABBIX

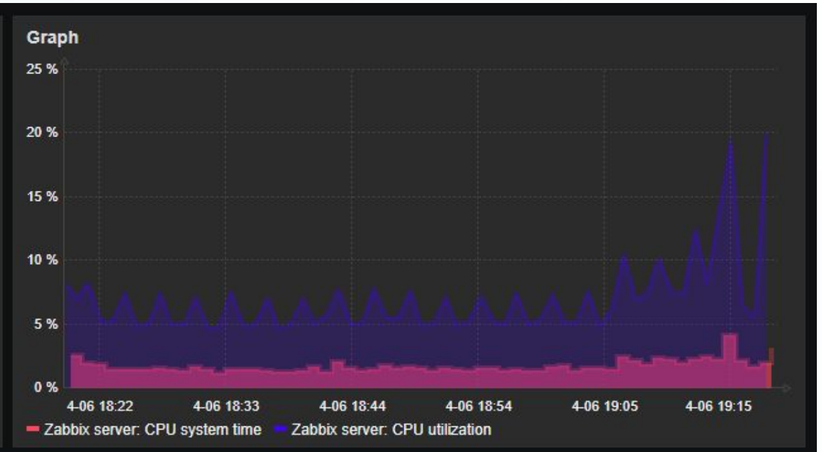


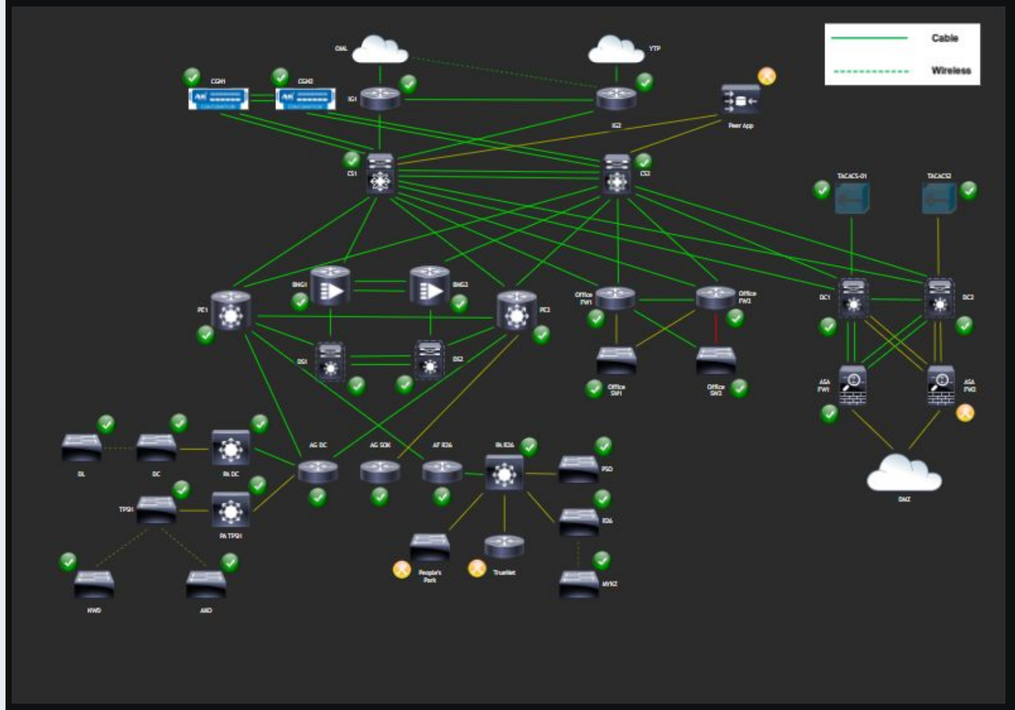
VISUALIZAÇÃO

ZABBIX









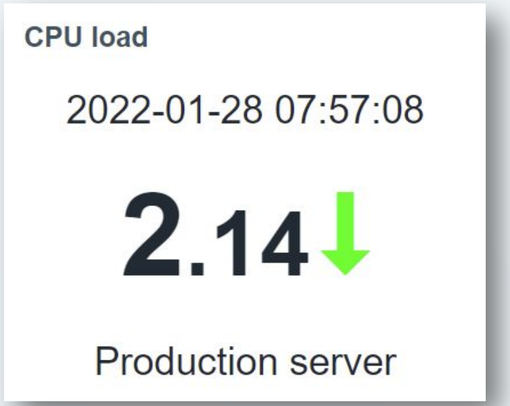
Problems by severity

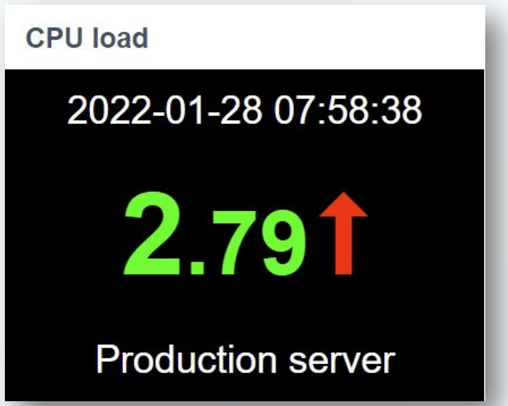
Host group ▲	Disaster	High	Average	Warning	Information	Not classified
New York Data center			16	1	1	
Oracle servers		1		4		
SNMP devices			14		1	

WIDGETS

ZABBIX

ITEM VALUE





WIDGETS

ZABBIX

TOP HOSTS

Top hosts by available memory

Host name	Available memory	Total memory
Database server	4.51 GB	31.25 GB
Production server	97.71 MB	7.81 GB
Web server	834.51 KB	3.91 GB

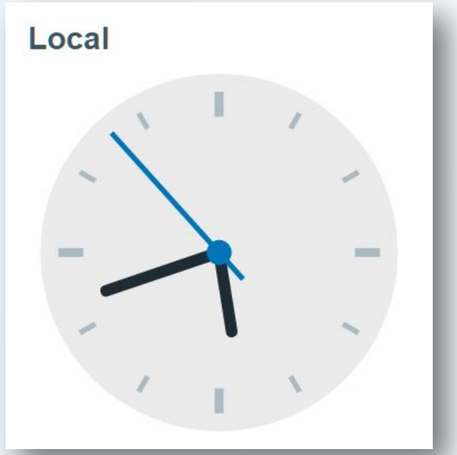
Top hosts by available memory

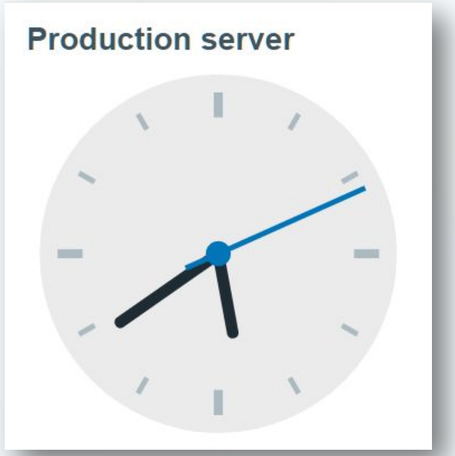
Host name	Available memory	Total memory
Database server		31.25 GB
Production server		7.81 GB
Web server		3.91 GB

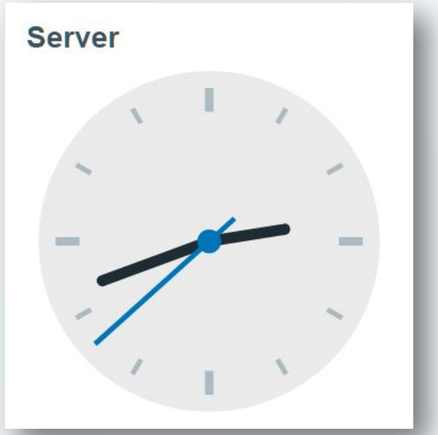
WIDGETS

ZABBIX

TOP HOSTS

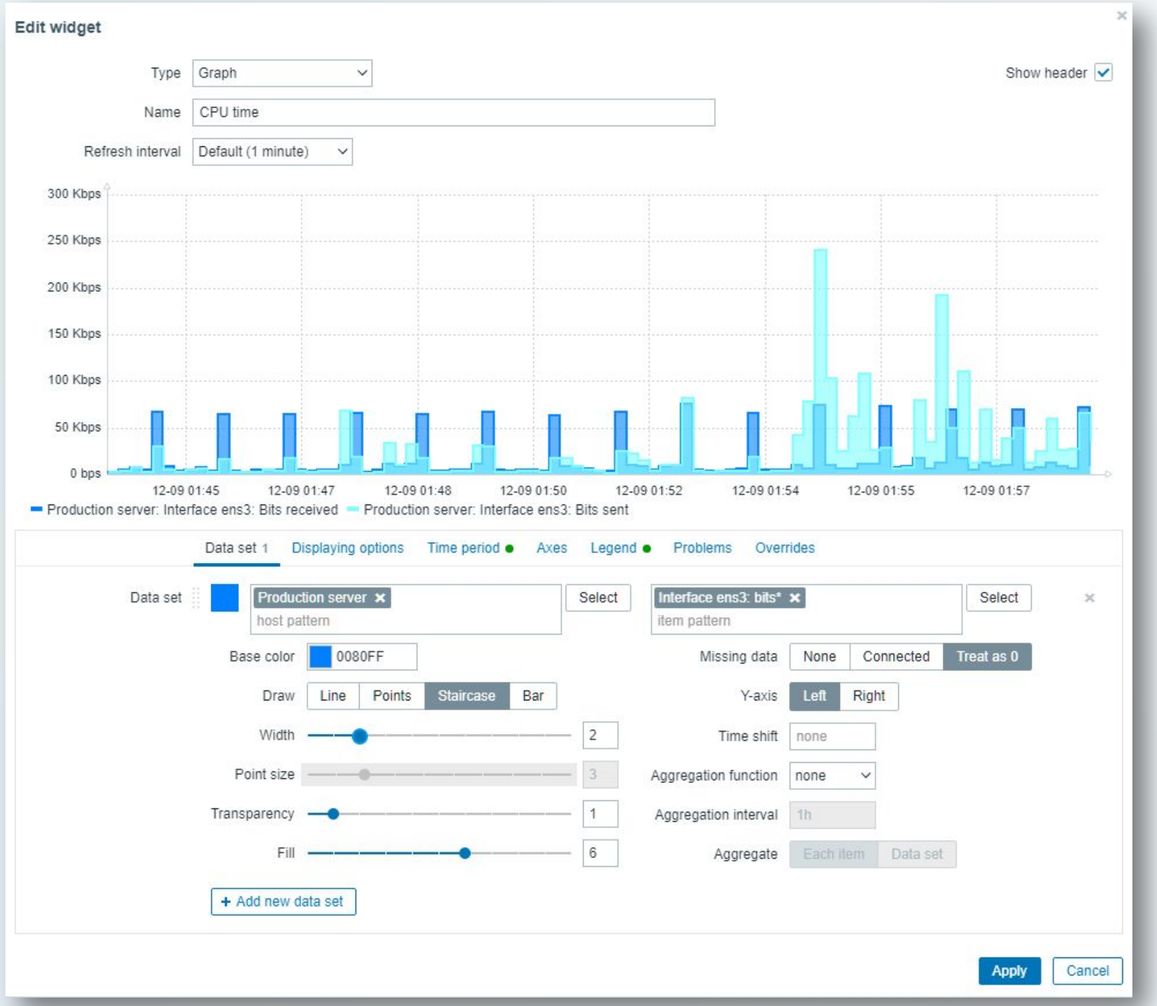


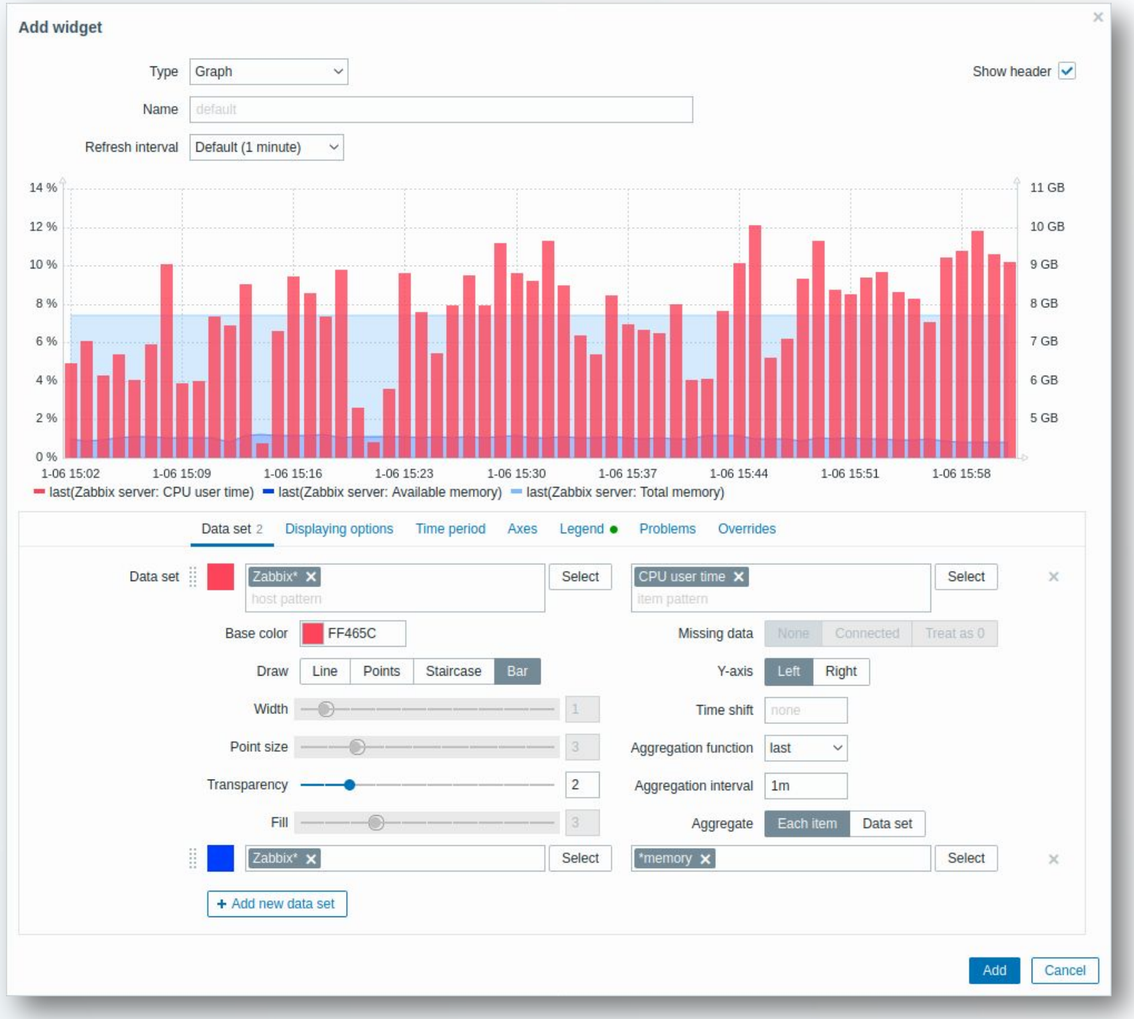




WIDGETS

GRÁFICOS





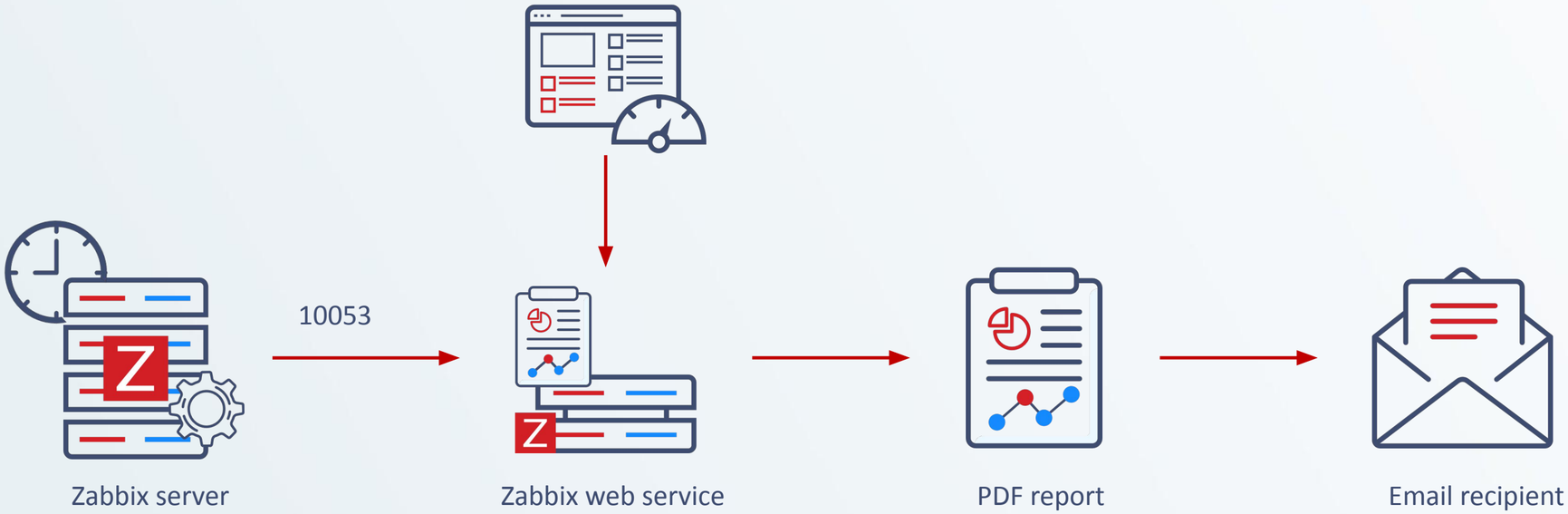
RELATÓRIOS AGENDADOS

ZABBIX

RELATÓRIOS EM PDF BASEADOS NOS DASHBOARDS

- **Para dashboards com múltiplas páginas, apenas a primeira página pode ser usada no relatório**

- **Possibilita o envio não só para usuários do Zabbix, mas para endereços externos**



MONITORAMENTO VIA SNMP

ZABBIX

ALGUNS PONTOS SOBRE O SNMP

- **S**imple **N**etwork **M**anagement **P**rotocol
- Coleta informações relacionadas à saúde e desempenho do dispositivo
- Operações suportadas:

Operação	Descrição da operação
GET	Retorna dados de um elemento presente em uma entidade da rede
GETNEXT	Retorna os dados subsequentes a um elemento de uma entidade da rede
SET	Envia configurações ou comandos de controle para uma entidade da rede
TRAP	Possibilita uma entidade da rede enviar notificações para a estação de gerência
INFORM	Uma trap reconhecida (a entidade da rede pode tentar reenviar a trap se nenhum reconhecimento for recebido (acknowledged trap))

MONITORAMENTO VIA SNMP

ZABBIX

ALGUNS PONTOS SOBRE O SNMP - VERSÕES

- **SNMPv1:**
  - Criado em meados dos anos 80
  - Fácil de configurar – Requer apenas uma string chamada “community“.
  - Muito vulnerável – informações são enviadas na rede em texto pleno

- **SNMPv2:**
  - Traz tudo o que a v1 tinha e inclui melhorias em performance, segurança e gerência
  - Introduz *GetBulkRequest*, comando *Inform* e suporte para contadores 64-bit
  - *Party-based security system* – muito complexo e amplamente não adotado 😢
  - SNMPv2c – Community-Based – Utiliza o esquema de segurança da v1

- **SNMPv3:**
  - Finalmente, segurança! x Mais complexo de configurar
  - Autenticação – para garantir que as mensagens sejam lidas apenas pelo recipiente desejado
  - Encriptação – Encripta as mensagens transferidas pela rede e garante que não possam ser lidas por usuários sem autorização

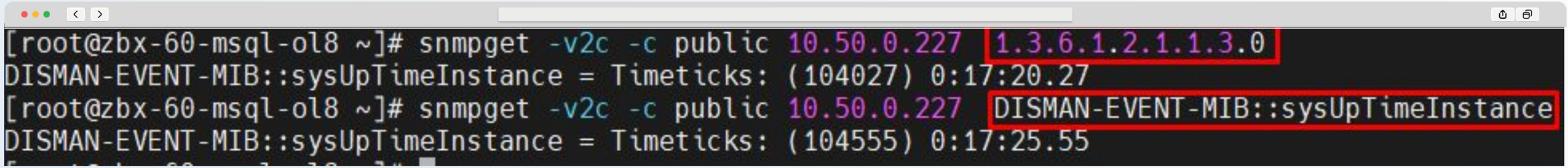
MONITORAMENTO VIA SNMP

ZABBIX

SUITE NET-SNMP

- É um pacote de ferramentas usadas para executar as operações do protocolo SNMP, e implementar SNMP v1, SNMP v2 e SNMP v3 utilizando IPv4 e IPv6

Operação	Comando	Descrição do comando
GET	snmpget	Utiliza a operação GET para retornar informações da entidade da rede
GETNEXT	snmpwalk	Utiliza a operação GETNEXT para consultar a árvore de informações de uma entidade da rede
SET	snmpset	Utiliza a operação SET para setar novas informações na entidade da rede
TRAP/INFORM	snmptrapd	Recebe e loga mensagens resultantes de operações TRAP e INFORM



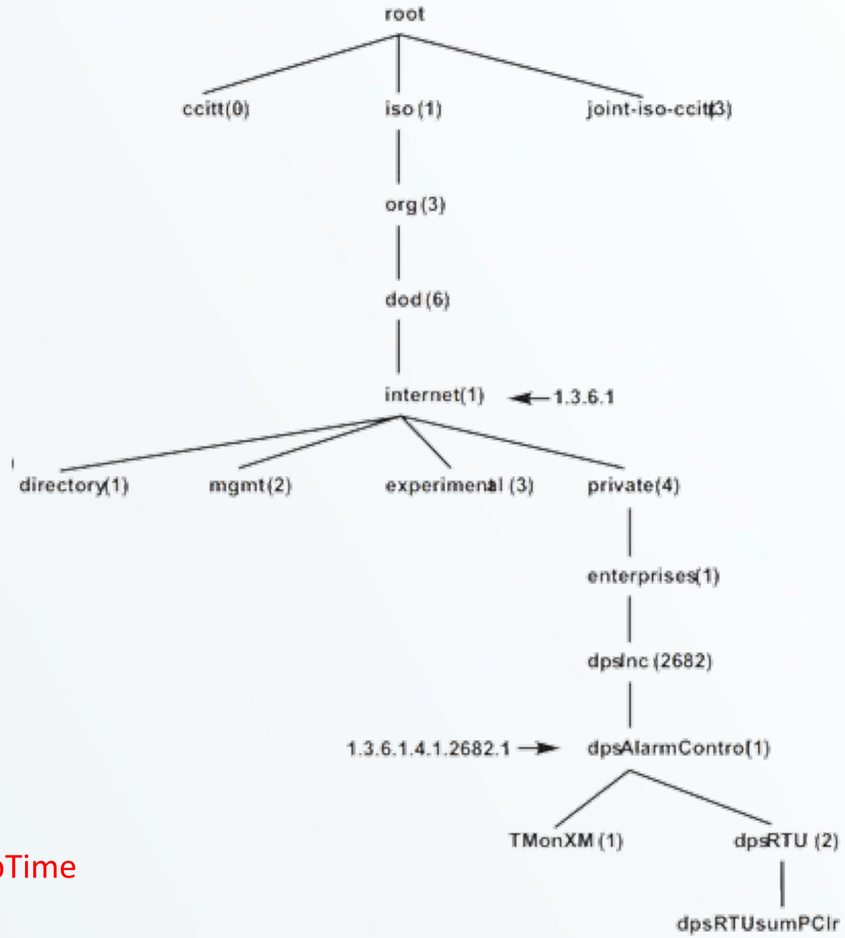
MONITORAMENTO VIA SNMP

ZABBIX

MIB E OID

- **MIB = M**anagement **I**nformation **B**ase
  - É um arquivo de texto com uma determinada formatação e organizado de forma hieráquica
  - Contem os detalhes dos **objetos** monitoráveis

- **OID = O**bject **Id**entifier
  - Endereço utilizado para diferenciar informações entre objetos
  - Representado por uma longa sequência de números separados por pontos



.1 iso
.1.3 org
.1.3.6 dod
.1.3.6.1 internet
.1.3.6.1.2 mgmt
.1.3.6.1.2.1 mib-2
.1.3.6.1.2.1.1 system
.1.3.6.1.2.1.1.1 sysDescr
.1.3.6.1.2.1.1.2 sysObjectID
.1.3.6.1.2.1.1.3 sysUpTime

1.3.6.1.2.1.1.3
=
iso.org.dod.internet.mgmt.mib-2.system.sysUpTime

MONITORAMENTO VIA SNMP

ZABBIX

Zabbix x SNMP

- O Zabbix envia um request SNMP GET para o dispositivo
- O dispositivo responde com um valor ou uma mensagem de erro
- A comunicação por padrão se dá através do protocolo UDP na porta 161

OID	Name
1.3.6.1.2.1.1.1	sysDescr
1.3.6.1.2.1.1.2	sysObjectID
1.3.6.1.2.1.1.3	sysUpTime
1.3.6.1.2.1.1.4	**sysContact**
1.3.6.1.2.1.1.5	sysName
1.3.6.1.2.1.1.6	sysLocation

MONITORAMENTO VIA SNMP

ZABBIX

Zabbix x SNMPTrap

- Situações de problemas ou limiares são definidos no dispositivo
- Cada tipo de dispositivo tem seus itens de trap únicos
- Quando um problema é identificado, ele enviará a mensagem SNMP para todos os recipientes configurados

ZABBIX

VAMOS VER NA PRÁTICA?