

The Zabbix logo consists of the word "ZABBIX" in white, uppercase, sans-serif font, centered within a solid red rectangular bar. The background of the entire slide is a dark blue gradient with a faint, glowing network of white lines and a subtle world map pattern.

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



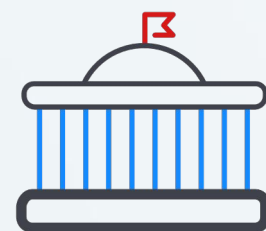
[in /in/victor-bc](https://www.linkedin.com/in/victor-bc)

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

ZABBIX

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

NO ANO SEGUINTE FOI ESTABELECIDADA 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?

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?

- **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)

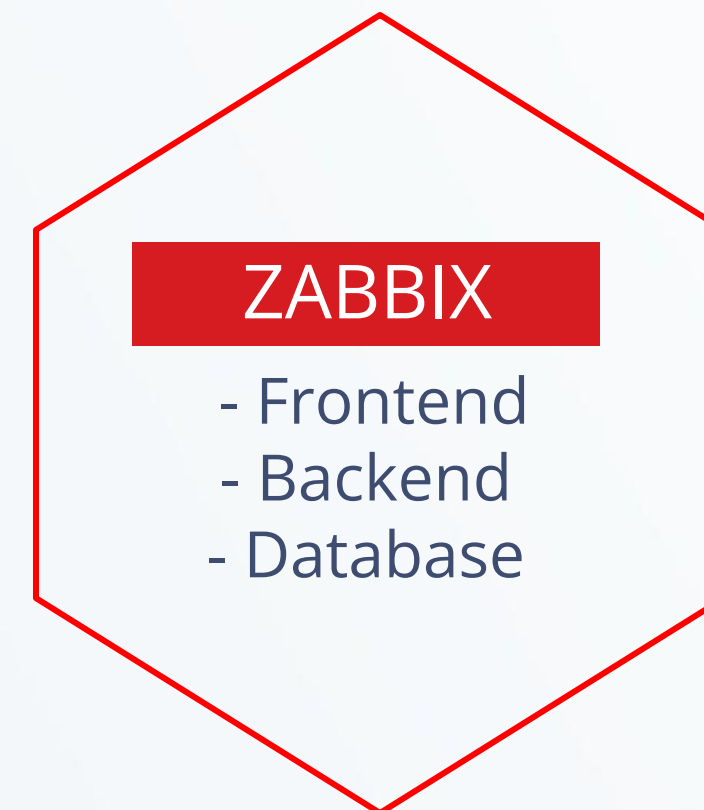
- Processo central responsável pela coleta e análise de dados

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)

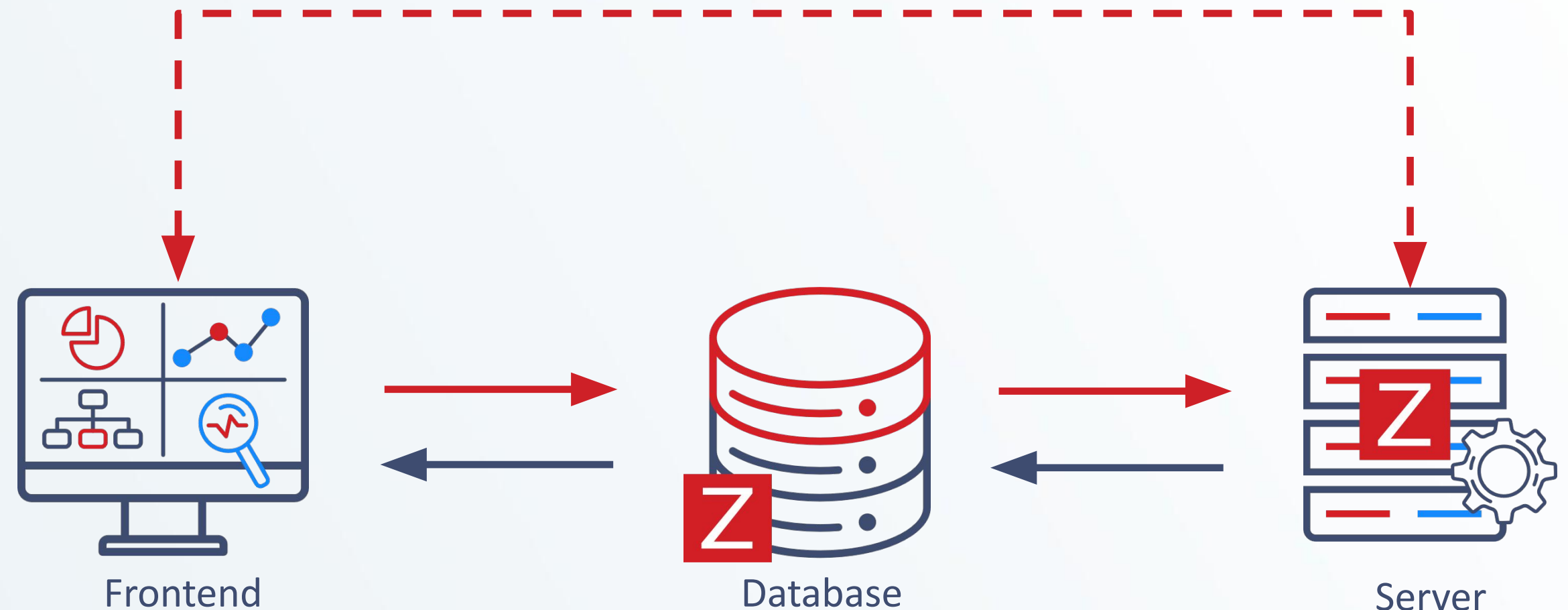
- Processo central responsável pela coleta e análise de dados

DATABASE

- Armazenamento de dados e configurações

FRONTEND

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



COMO FUNCIONA?

ZABBIX SERVER (BACKEND)

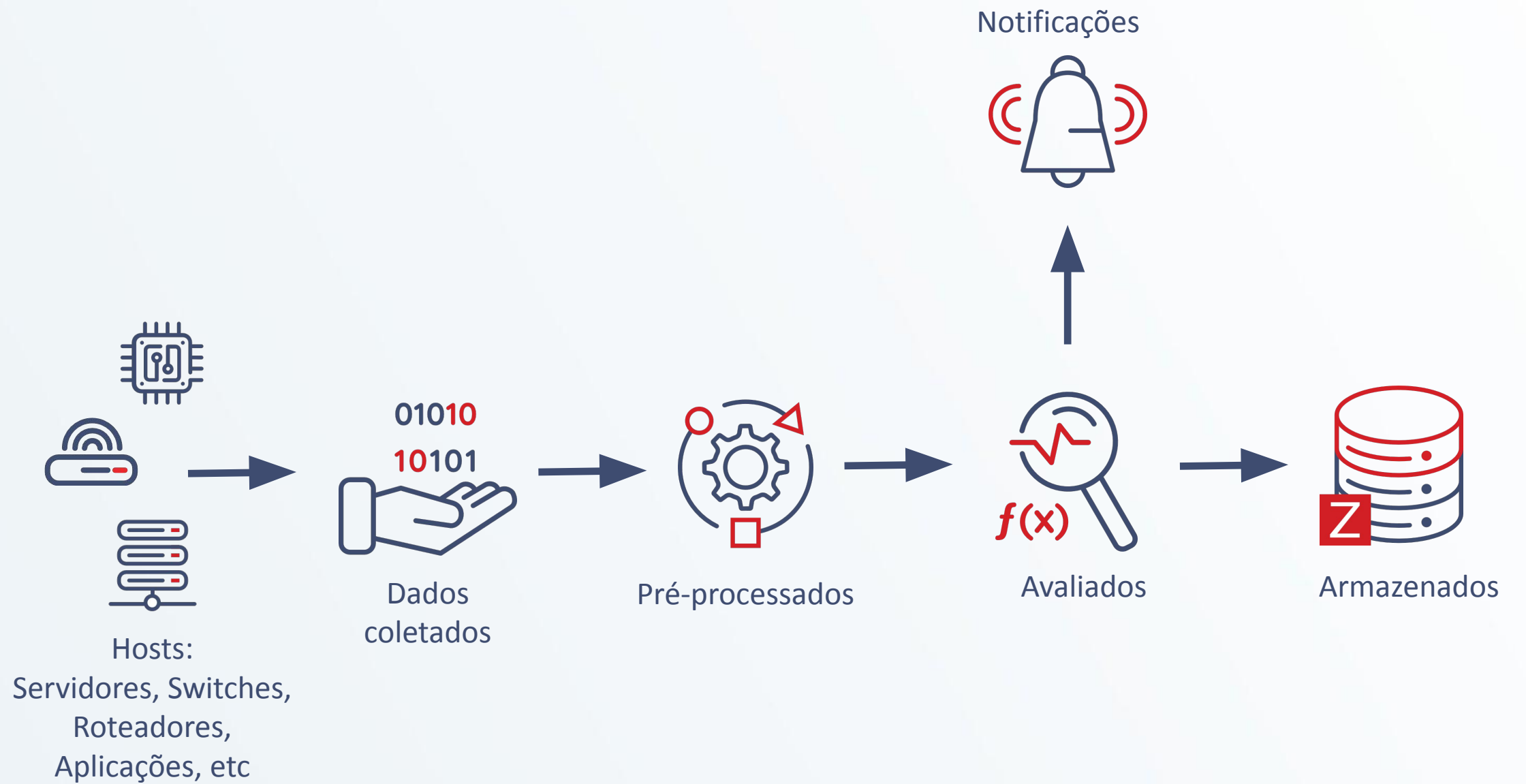
- Processo central responsável pela coleta e análise de dados

DATABASE

- Armazenamento de dados e configurações

FRONTEND

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

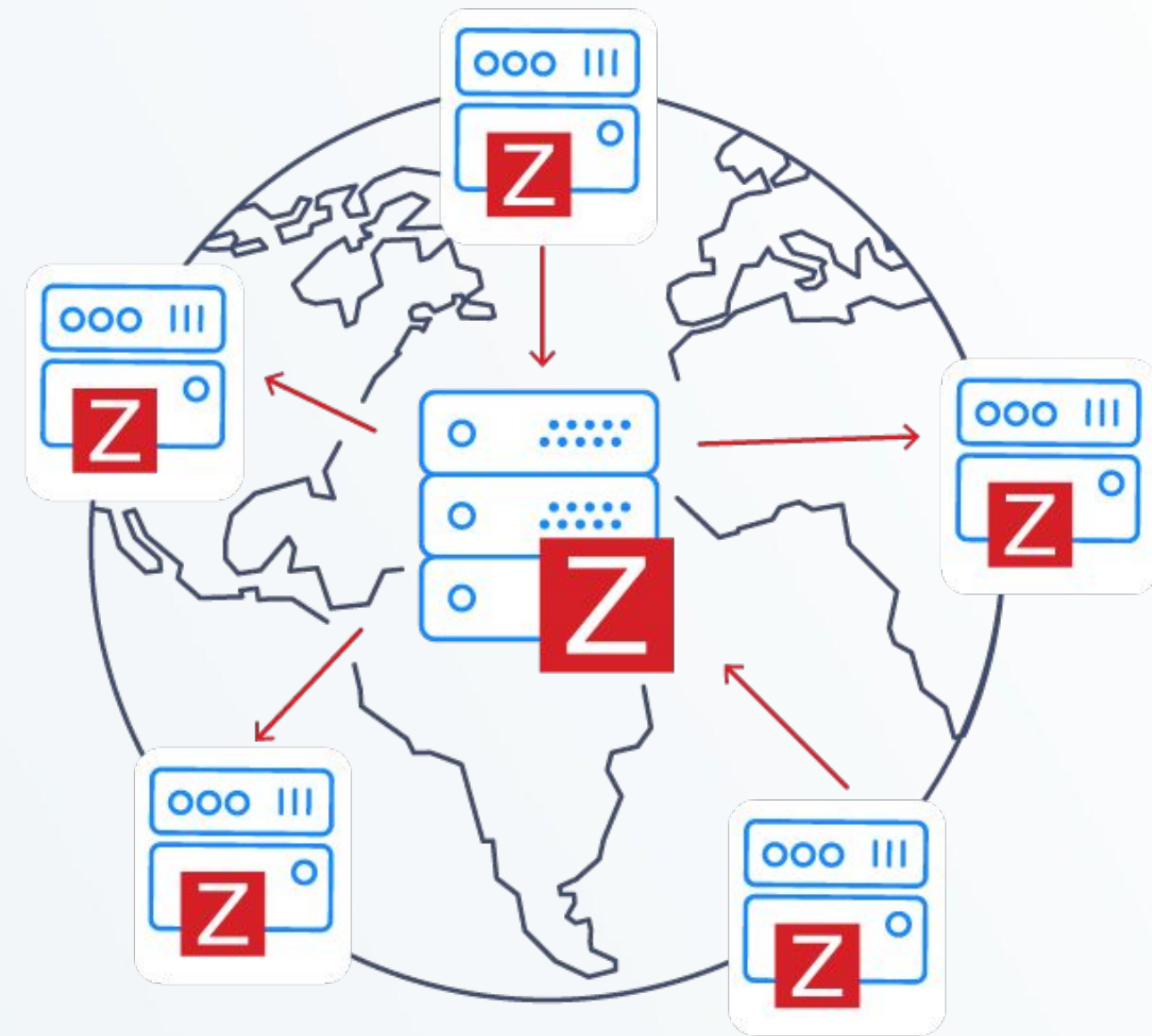


MONITORAMENTO DISTRIBUÍDO

ZABBIX

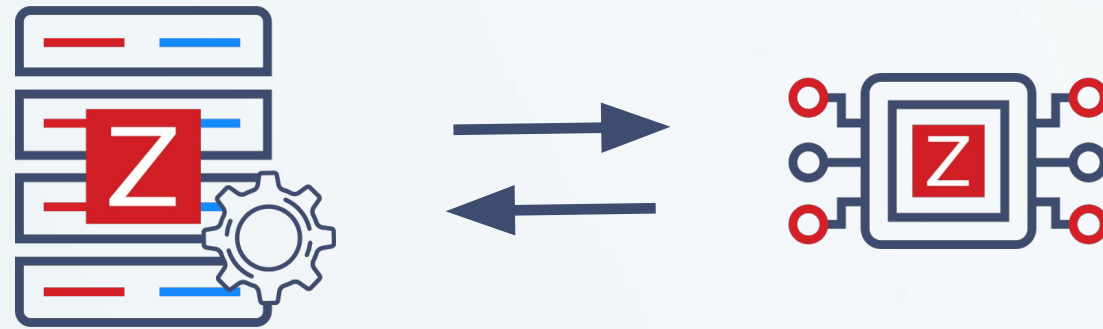
Zabbix proxies em locais remotos para redundância e fácil configuração

- 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

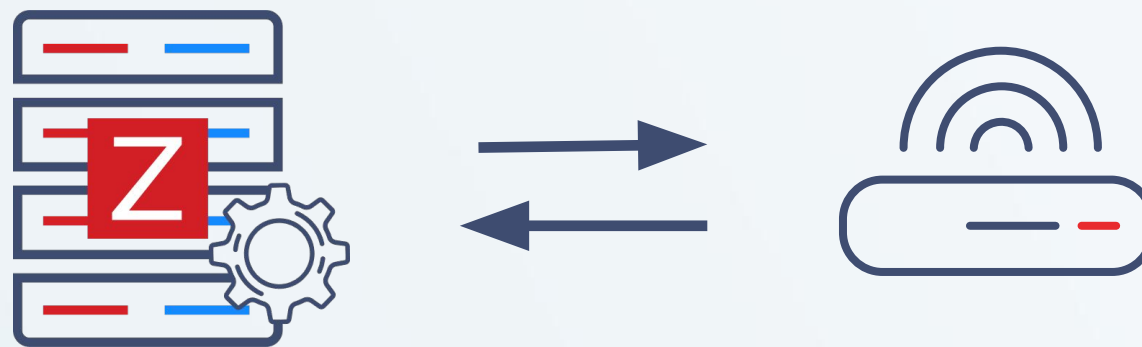


COLETA DOS DADOS

- ATRAVÉS DE UM AGENTE



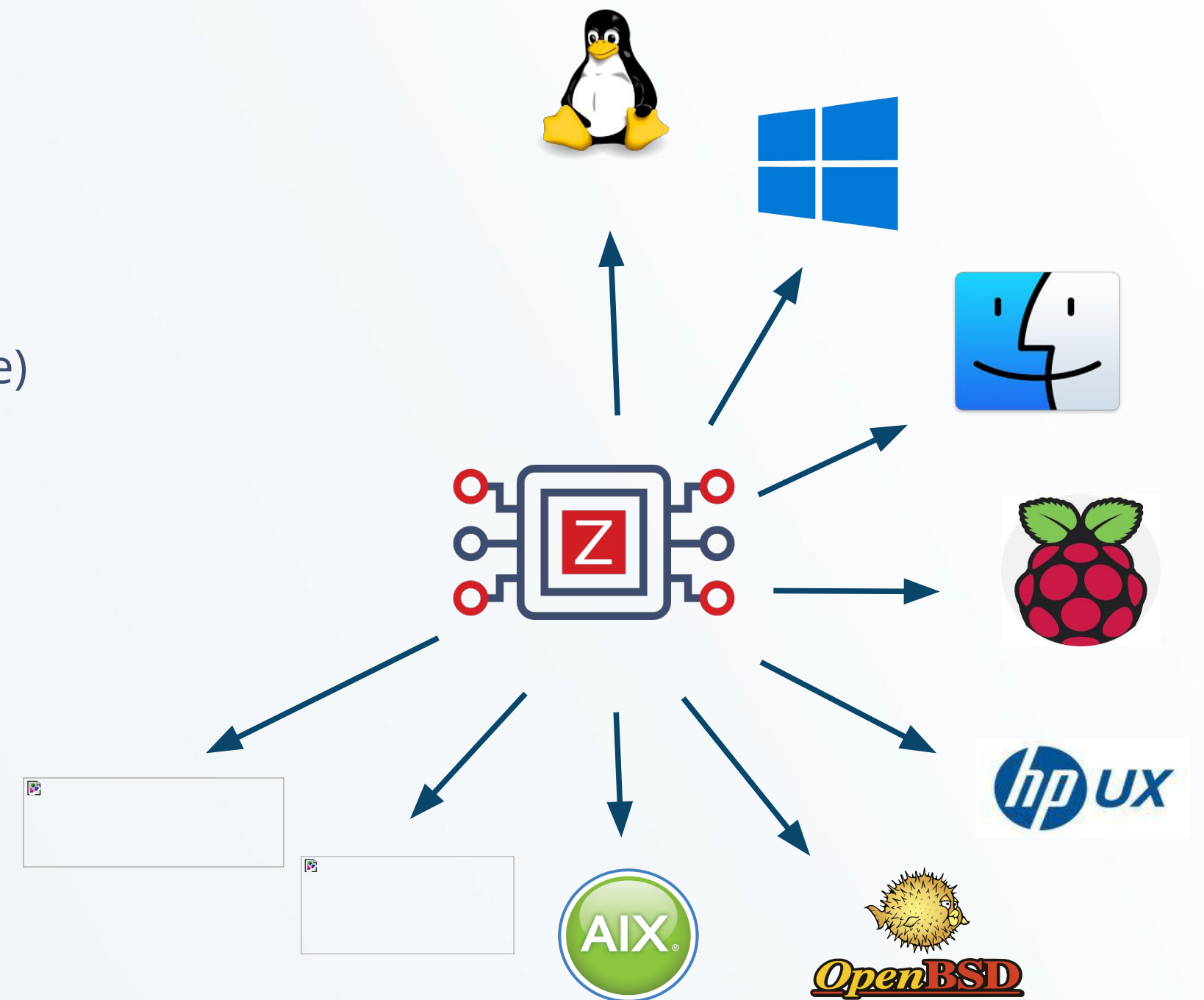
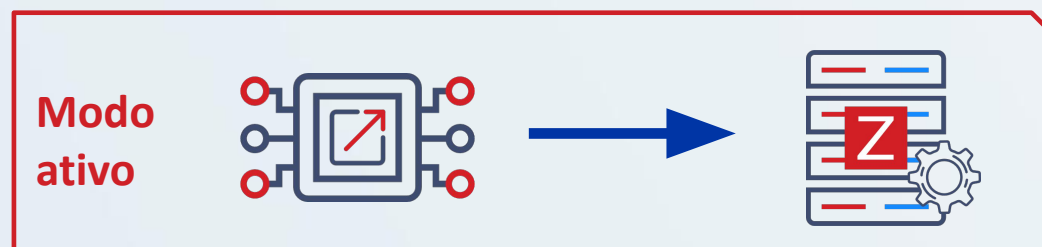
- SEM AGENTE (AGENTLESS)



COLETA DOS DADOS

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

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

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...

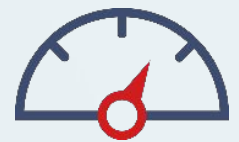
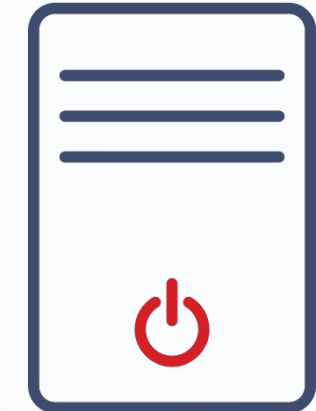


CONCEITOS BÁSICOS

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

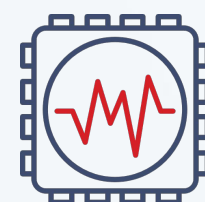
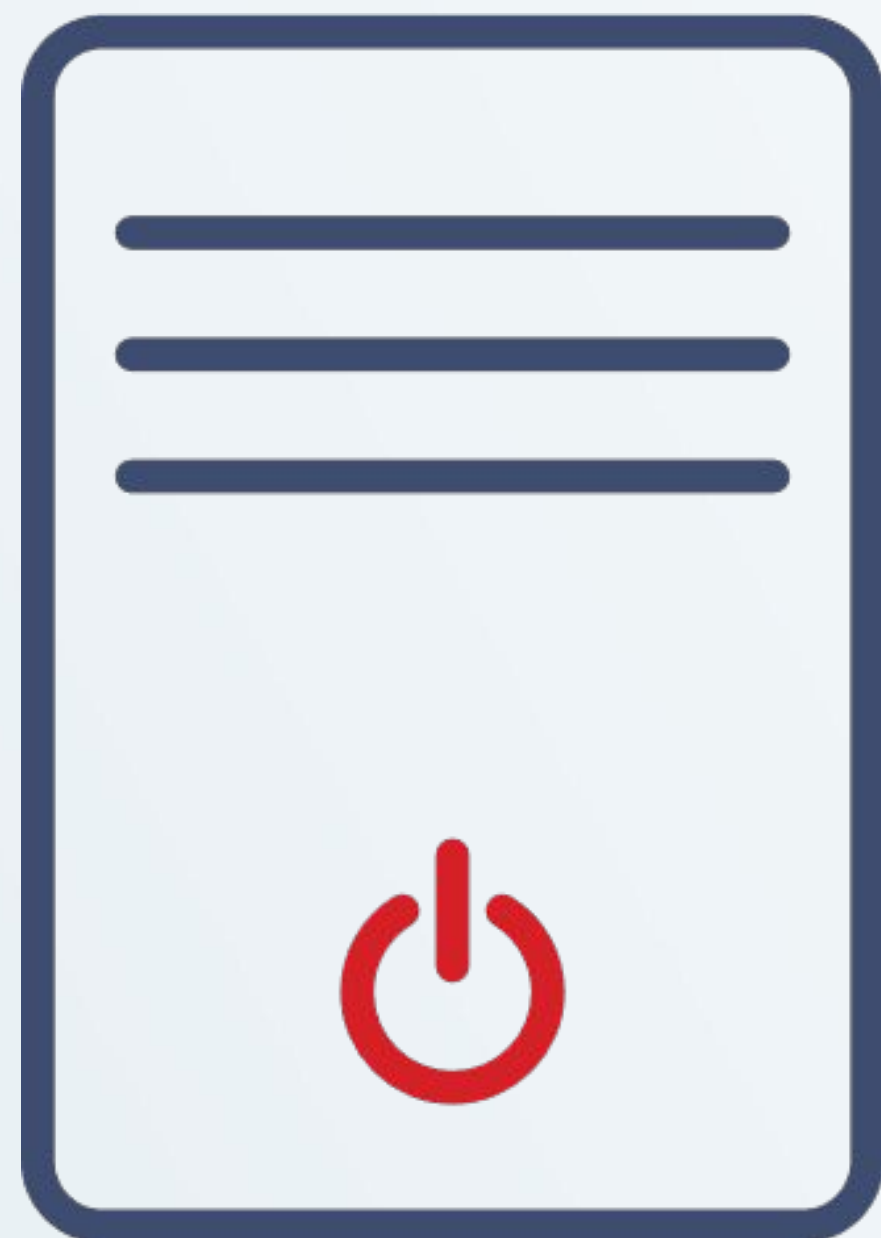
- **Action**

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)



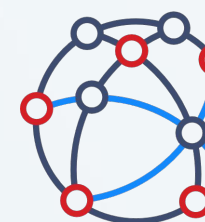
Items



Triggers



Gráficos



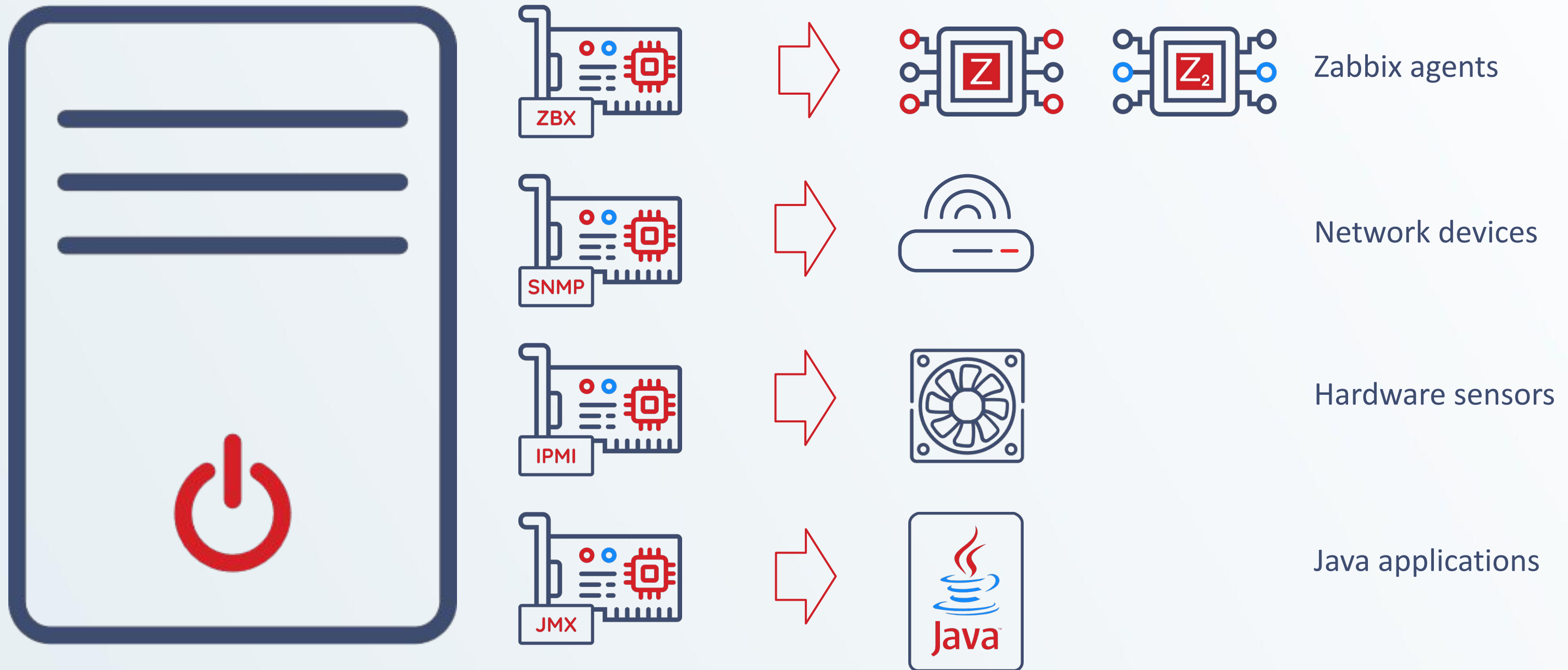
Cenários Web



Regras de descoberta de baixo nível
(LLD)

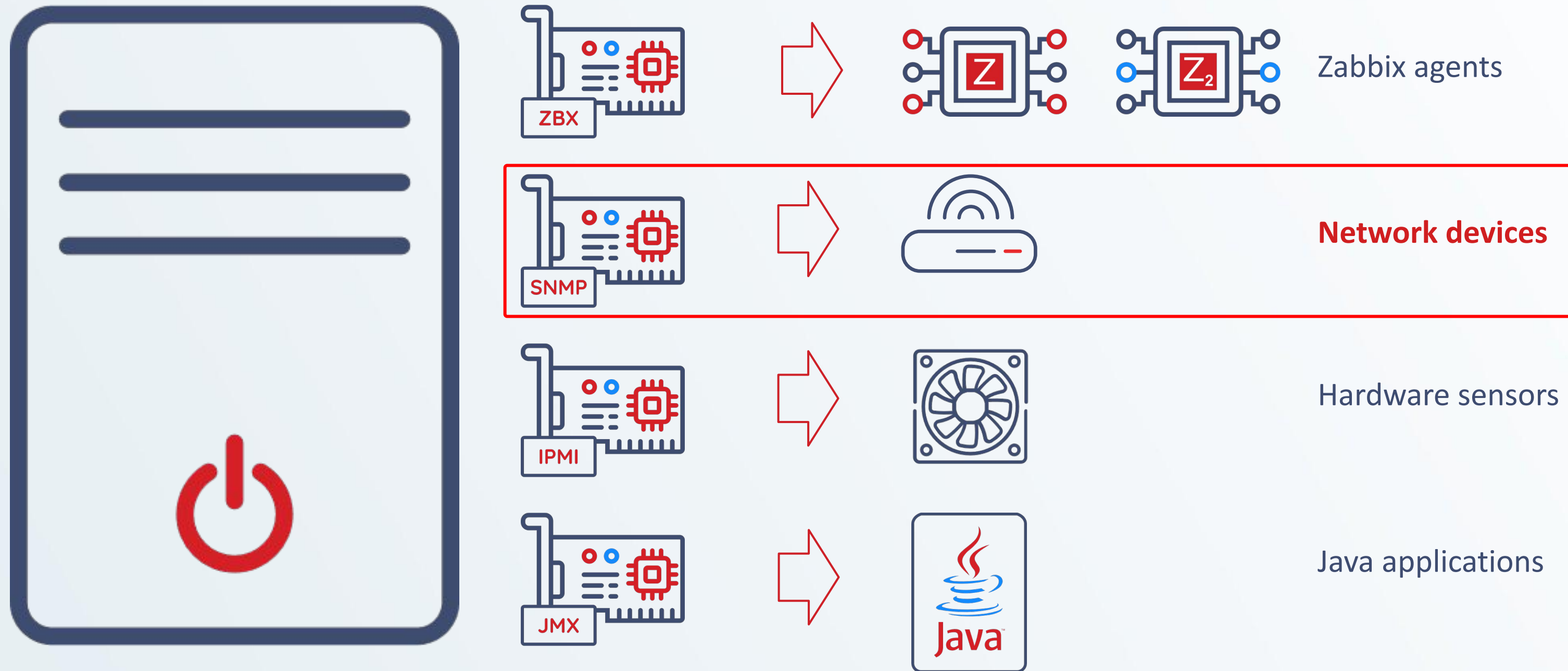
INTERFACES DO HOST

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



INTERFACES DO HOST

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



INTERFACES DO HOST

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

* SNMP version	SNMPv1	▼
* SNMP community		
* SNMP version	SNMPv2	▼
* SNMP community	{\${SNMP_COMMUNITY}}	

SNMPv3 oferece demais parâmetros de segurança

* SNMP version	SNMPv3	▼
Context name		
Security name	zabbix	
Security level	authNoPriv	▼
Authentication protocol	SHA384	▼
Authentication passphrase	{\${SNMP.AUTHENTICATION}}	

ITEMS

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

The screenshot shows the Zabbix web interface for configuring a new item. The item is named "Available memory" and is of type "Zabbix agent". The key is "vm.memory.size[available]". The host interface is "127.0.0.1:10050". The type of information is "Numeric (unsigned)" and the units are "B". The update interval is "1m". There is a custom interval table with one entry: "Flexible Scheduling" with an interval of "50s" and a period of "1-7,00:00-24:00". The history storage period is "Storage period" with a value of "7d". The trend storage period is "Storage period" with a value of "365d". The value mapping field is empty. The "Populates host inventory field" is set to "-None-". The description is "Available memory = free + buffers + cache. On other platforms calculation may vary. See also: https://www.zabbix.com/documentation/6.0/manual/appendix/items/vm.memory.size_params". The "Enabled" checkbox is checked. At the bottom, there are buttons for "Add", "Test", and "Cancel".

Type	Interval	Period	Action
Flexible Scheduling	50s	1-7,00:00-24:00	Remove

ITEMS

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

The screenshot shows the 'Preprocessing' tab of the Zabbix web interface for configuring a new item. The configuration is as follows:

- Name:** Available memory
- Type:** Zabbix agent
- Key:** vm.memory.size[available] (with a 'Select' button)
- Host interface:** 127.0.0.1:10050
- Type of information:** Numeric (unsigned)
- Units:** B
- Update interval:** 1m
- Custom intervals:** A table with columns for Type, Interval, Period, and Action. One entry is shown: Type: Flexible, Interval: Scheduling, Interval: 50s, Period: 1-7,00:00-24:00, Action: Remove. There is an 'Add' button below the table.
- History storage period:** Do not keep history (selected) and Storage period: 7d
- Trend storage period:** Do not keep trends (selected) and Storage period: 365d
- Value mapping:** type here to search (with a 'Select' button)
- Populates host inventory field:** -None-
- Description:** Available memory = free + buffers + cache. On other platforms calculation may vary. See also: https://www.zabbix.com/documentation/6.0/manual/appendix/items/vm.memory.size_params
- Enabled:**

At the bottom, there are three buttons: 'Add', 'Test', and 'Cancel'.

ITEMS

Item Tags 1 Preprocessing

* Name

Type

* Key

* Host interface

Type of information

Units

* Update interval

Custom intervals

Type	Interval	Period	Action
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	Remove

[Add](#)

* History storage period Storage period

* Trend storage period Storage period

Value mapping

Populates host inventory field

Description

Enabled

TRIGGER

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`

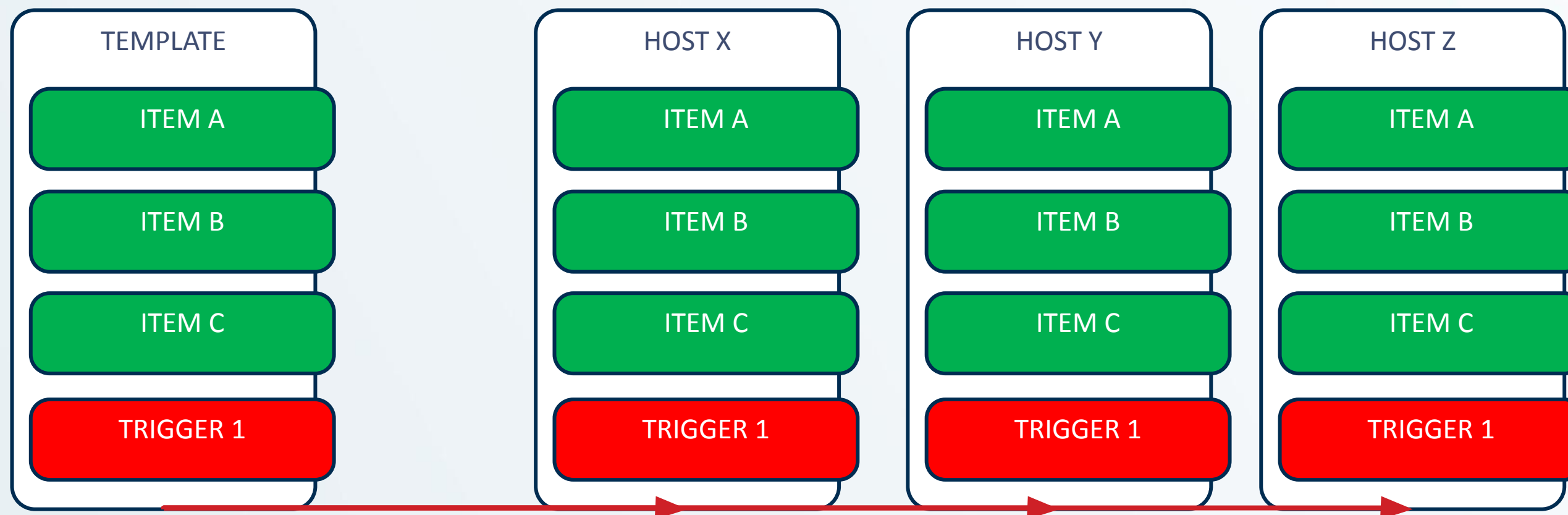
- Caso essa expressão seja **VERDADEIRA**, a trigger assume o estado de **PROBLEMA**

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

TEMPLATE

Conjunto de entidades que pode ser aplicado a múltiplos hosts

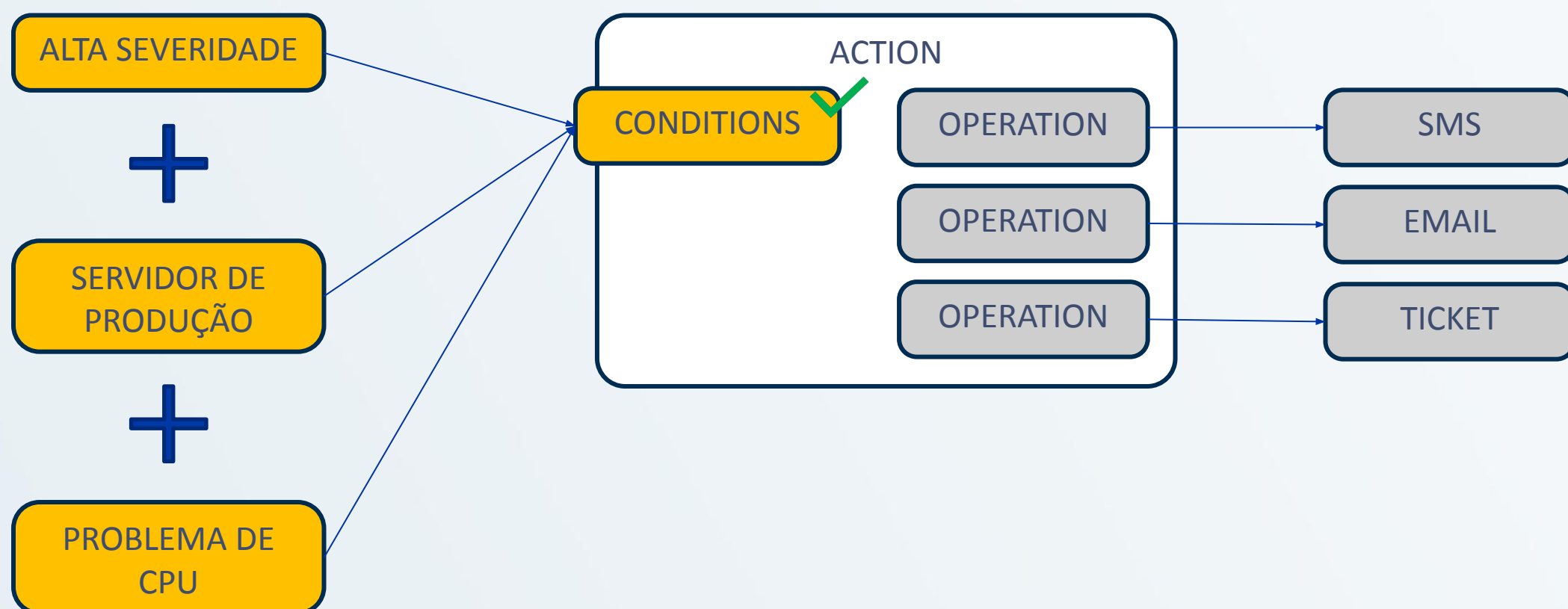
- Agilidade
- Simplicidade
- Facilidade de gerência de centenas/milhares de Hosts



Linkagem

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

ZABBIX

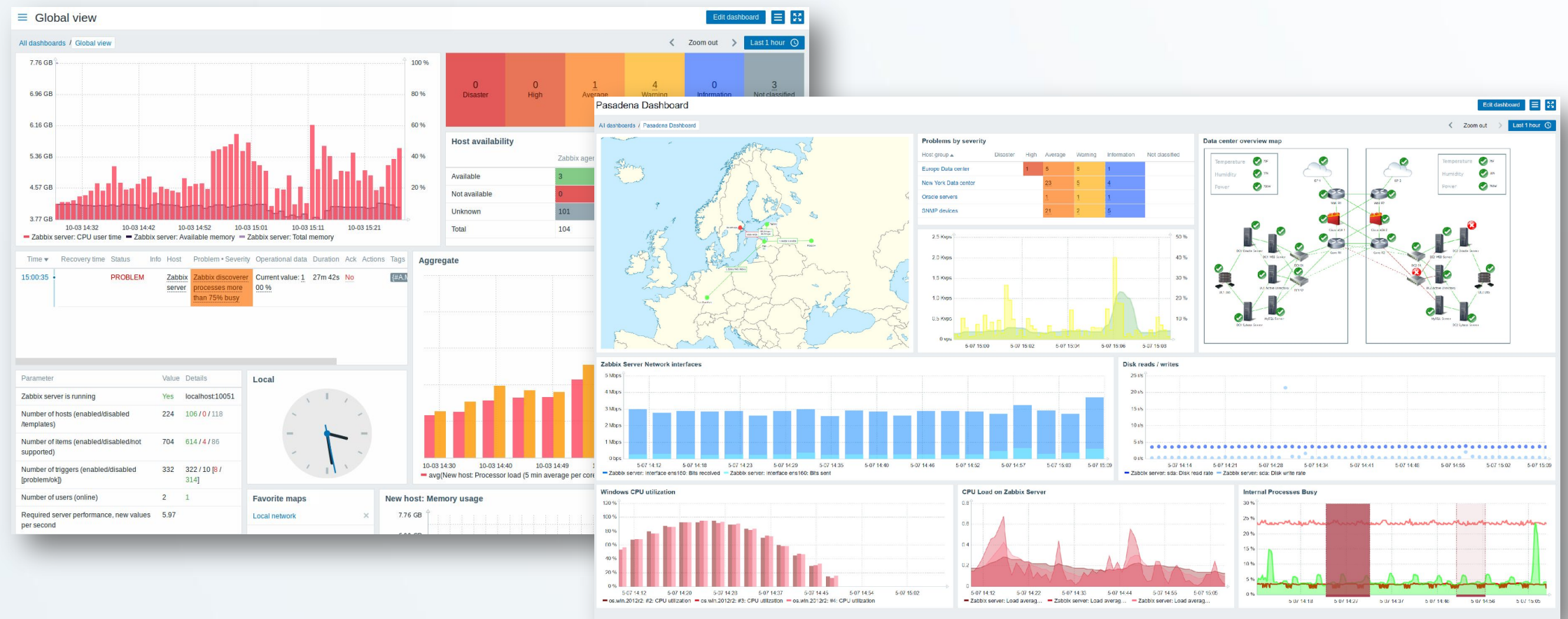
Através de Dashboards é possível visualizar um resumo de sua operação

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

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

VISUALIZAÇÃO - DASHBOARDS

ZABBIX

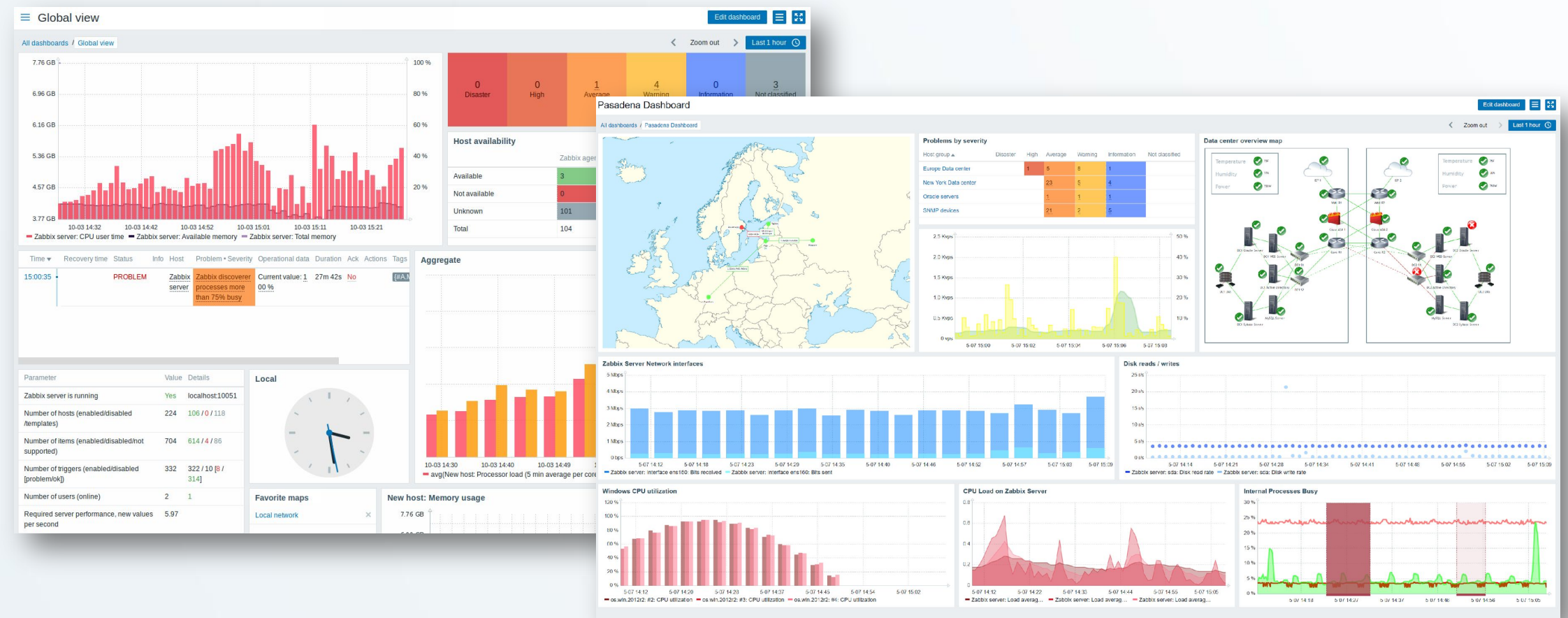
Através de Dashboards é possível visualizar um resumo de sua operação

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

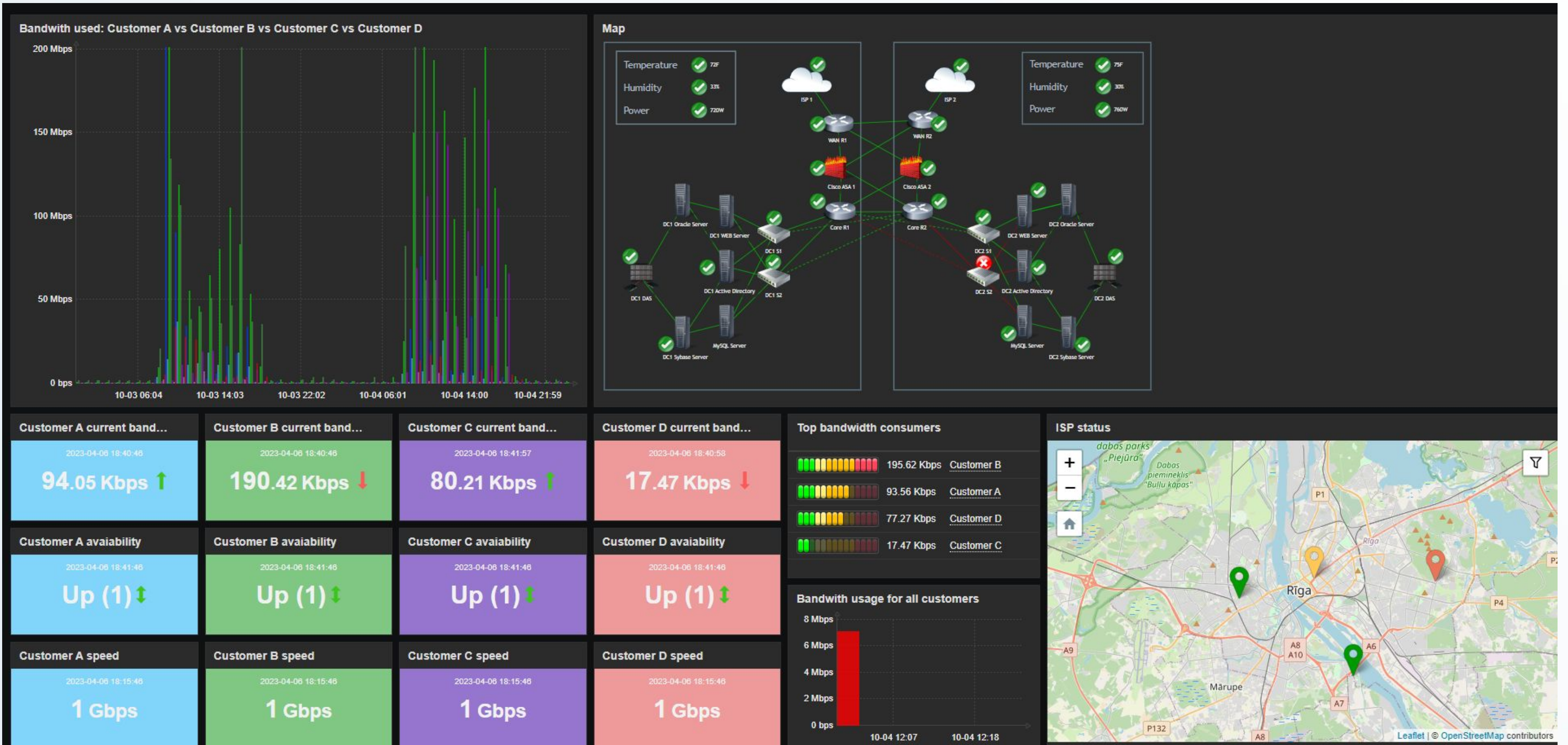
Exemplos de Widgets:

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



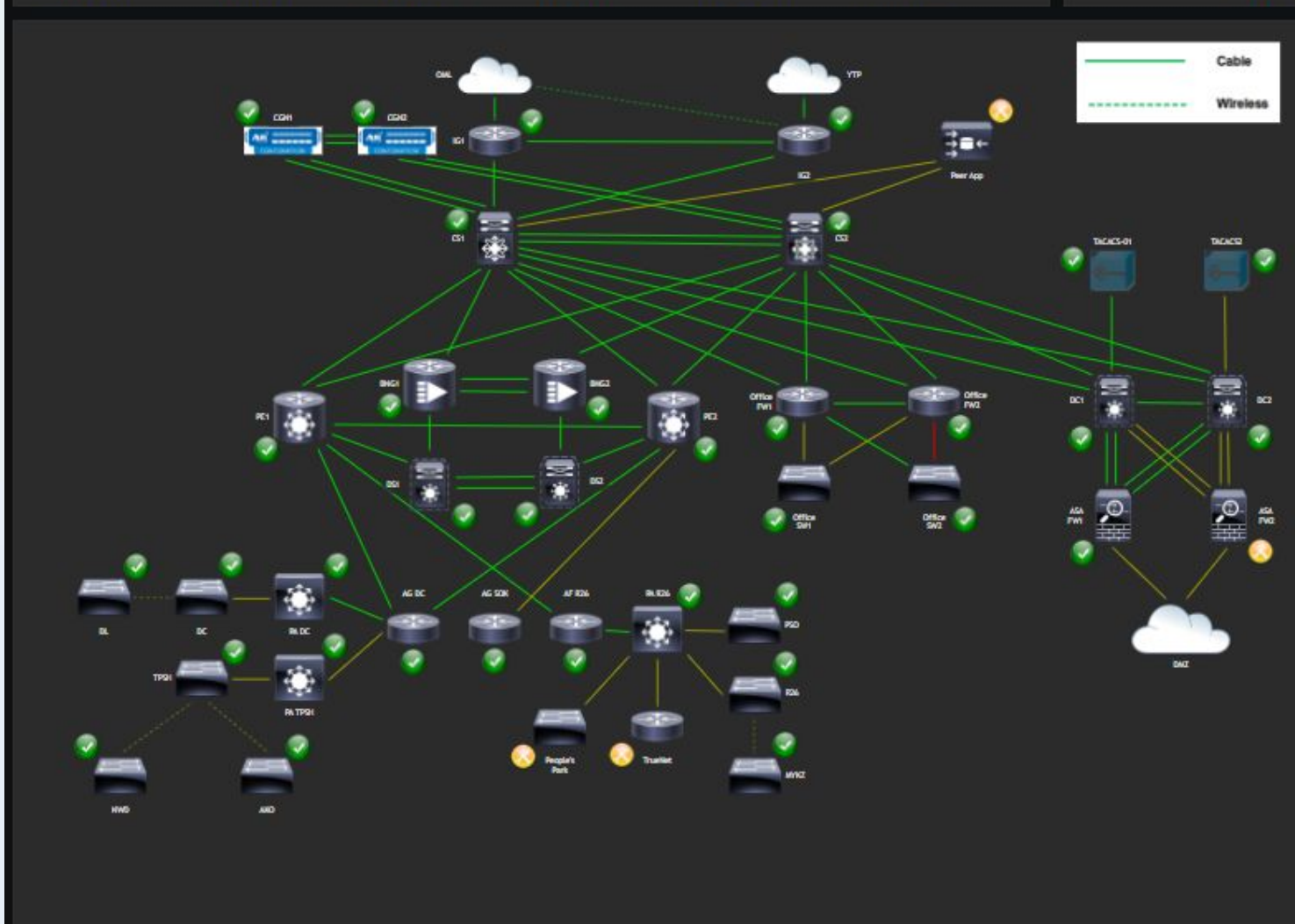
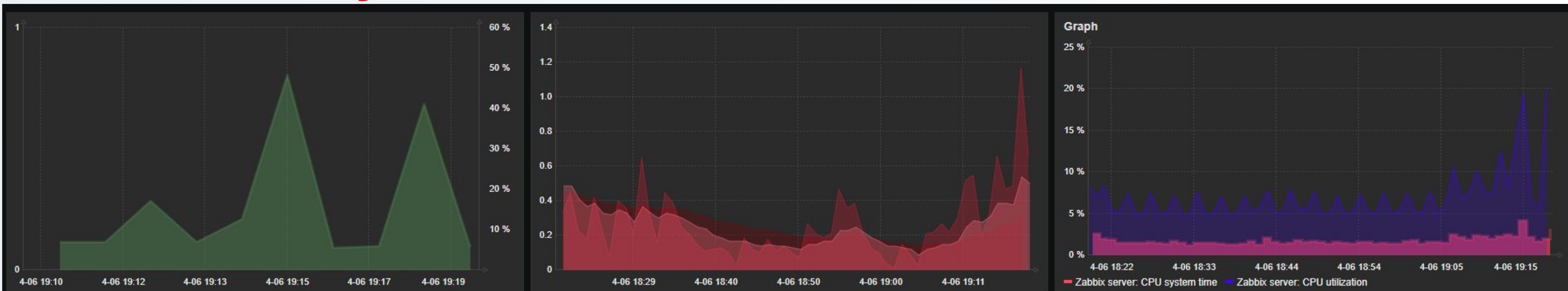
VISUALIZAÇÃO

ZABBIX



VISUALIZAÇÃO

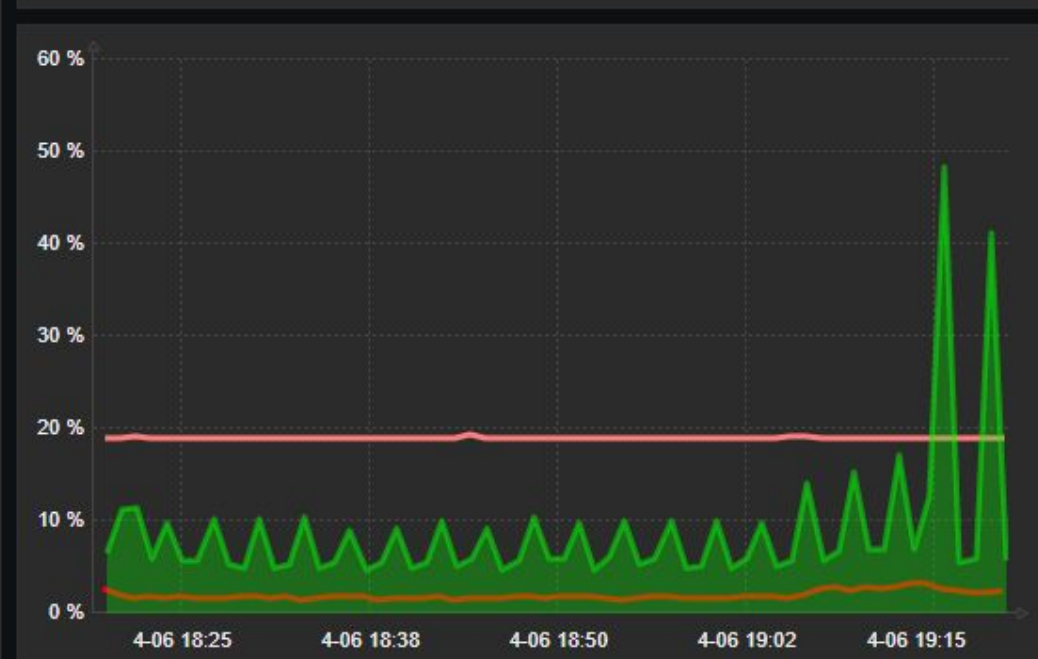
ZABBIX



Problems by severity

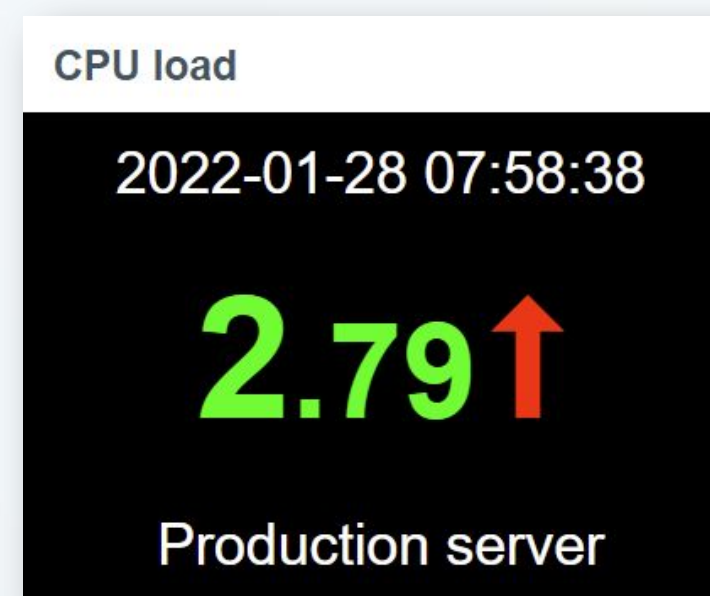
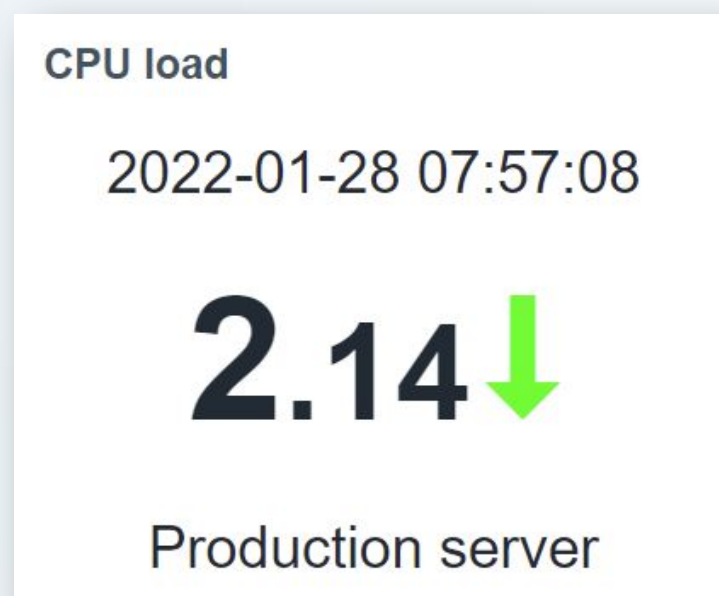
Host group ▲

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

ITEM VALUE






WIDGETS

TOP HOSTS

Top hosts by available memory

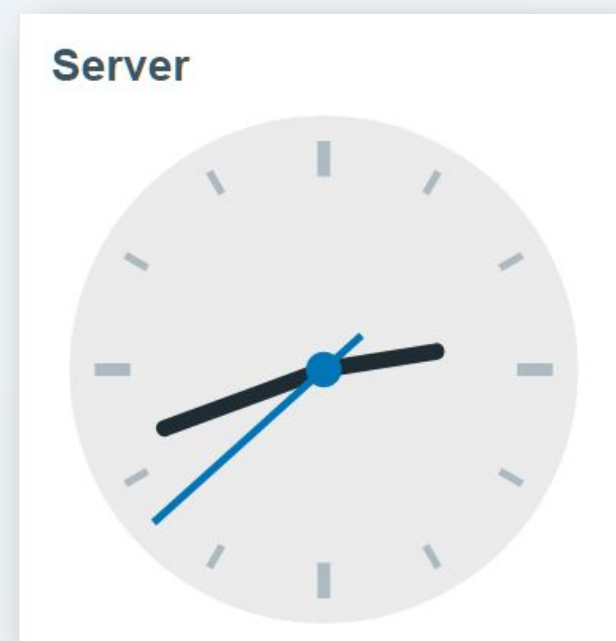
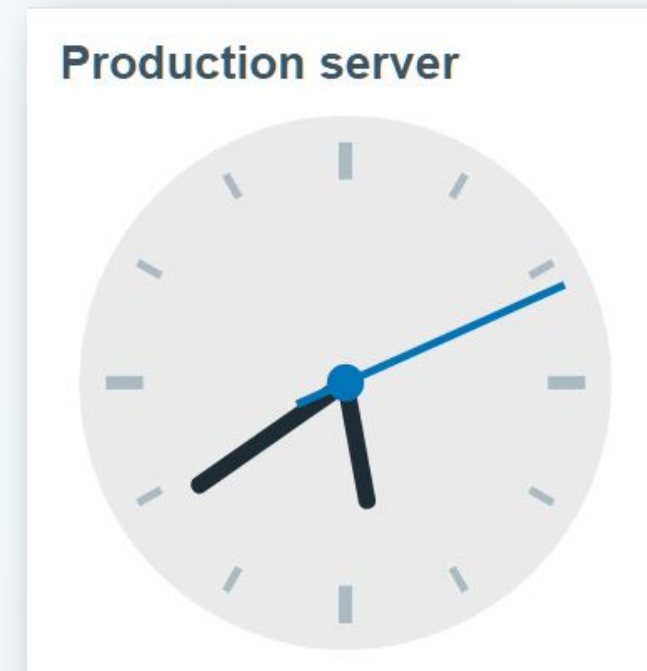
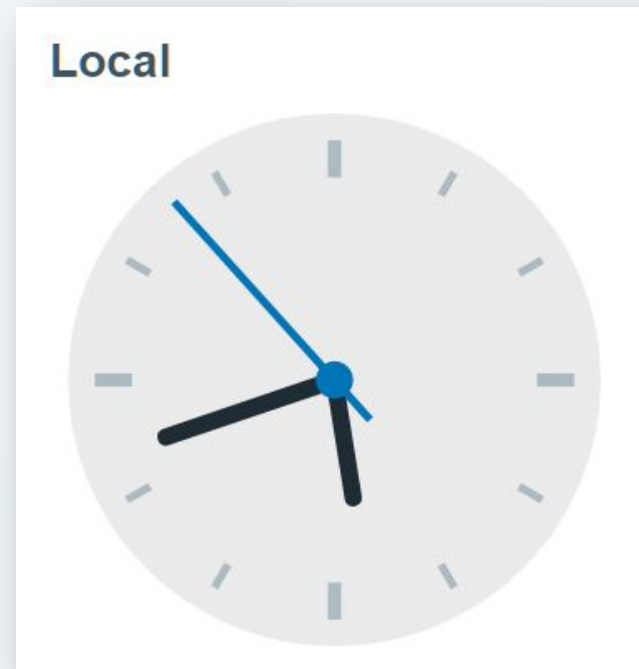
Host name	Available memory	Total memory
Database server	4.51 GB	31.25 GB
Production server	97.71 MB	7.81 GB
Web server	834.51 KB	3.91 GB

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

TOP HOSTS



WIDGETS

GRÁFICOS

Edit widget

Type: Graph Show header

Name: CPU time

Refresh interval: Default (1 minute)

■ Production server: Interface ens3: Bits received ■ Production server: Interface ens3: Bits sent

Data set 1 | Displaying options | Time period | Axes | Legend | Problems | Overrides

Data set: Production server (host pattern) | Interface ens3: bits* (item pattern)

Base color: 0080FF | Missing data: None | Connected | Treat as 0

Draw: Line | Points | Staircase | Bar

Width: 2 | Y-axis: Left | Right

Point size: 3 | Time shift: none

Transparency: 1 | Aggregation function: none

Fill: 6 | Aggregation interval: 1h

Aggregate: Each item | Data set

+ Add new data set

Apply Cancel

Add widget

Type: Graph Show header

Name: default

Refresh interval: Default (1 minute)

■ last(Zabbix server: CPU user time) ■ last(Zabbix server: Available memory) ■ last(Zabbix server: Total memory)

Data set 2 | Displaying options | Time period | Axes | Legend | Problems | Overrides

Data set: Zabbix* (host pattern) | CPU user time (item pattern)

Base color: FF465C | Missing data: None | Connected | Treat as 0

Draw: Line | Points | Staircase | Bar

Width: 1 | Y-axis: Left | Right

Point size: 3 | Time shift: none

Transparency: 2 | Aggregation function: last

Fill: 3 | Aggregation interval: 1m

Aggregate: Each item | Data set

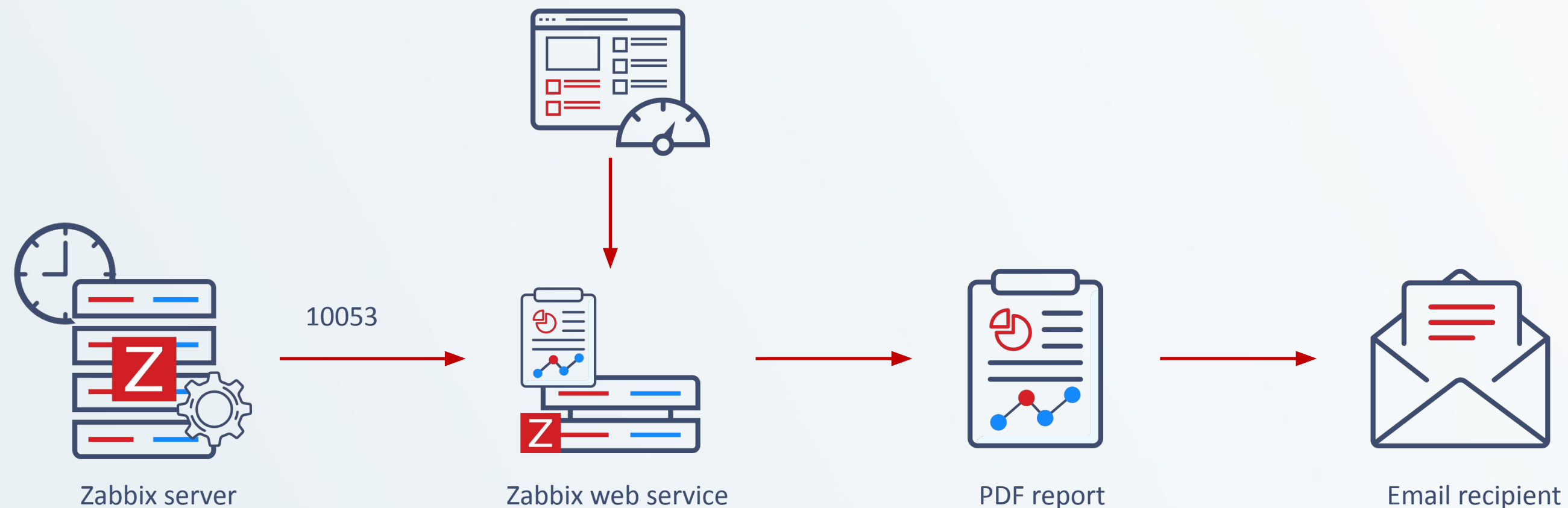
+ Add new data set

Add Cancel

RELATÓRIOS AGENDADOS

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

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

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

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

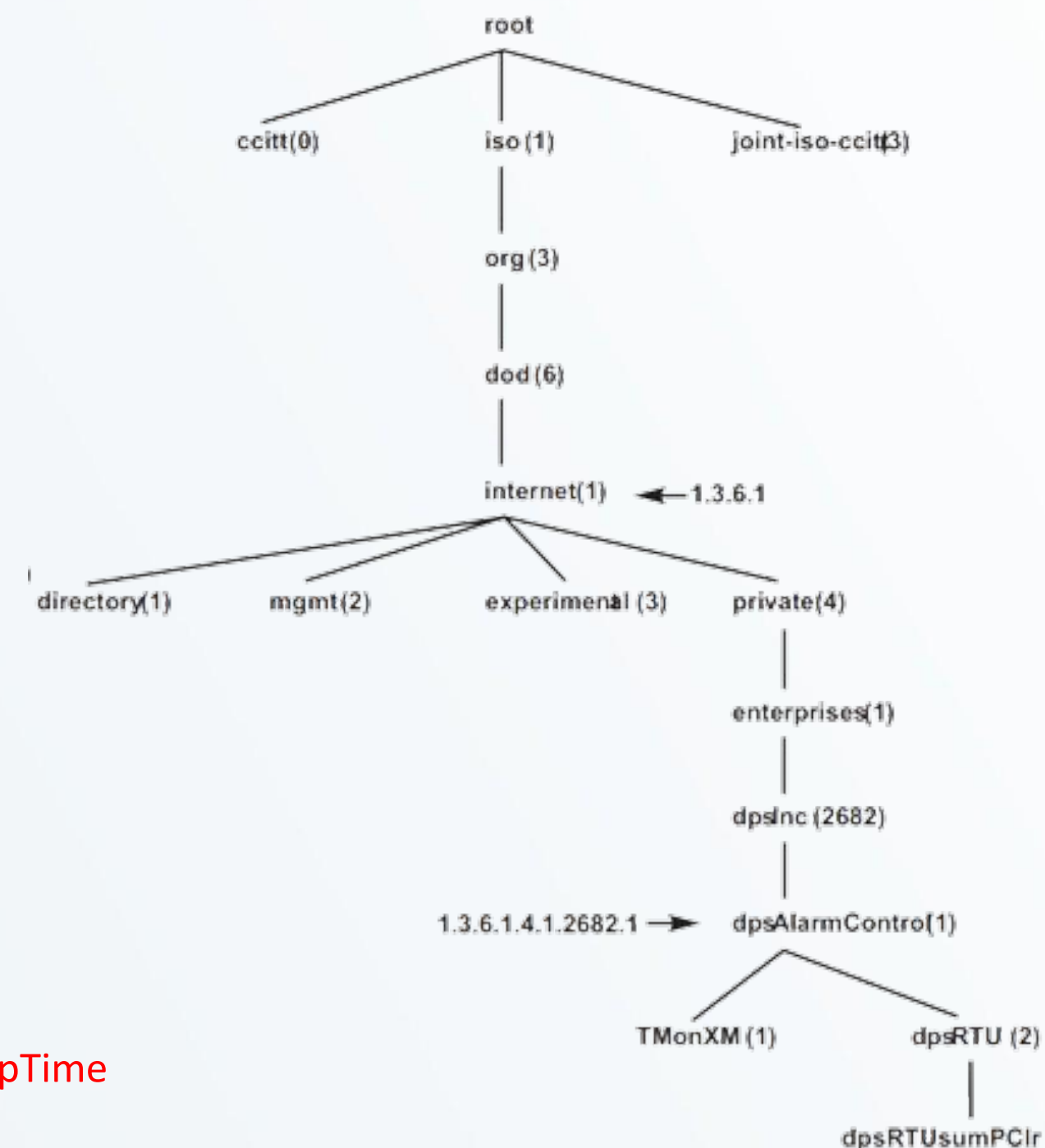
Operação	Comando	Descrição do comando
GET	snmpget	Utiliza a operação GET para retornar informações da entidade da rede
GETNEXT	snmpwalk	Utiliza a operação GETNEXT para consultar a árvore de informações de uma entidade da rede
SET	snmpset	Utiliza a operação SET para setar novas informações na entidade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

```
[root@zbx-60-mysql-ol8 ~]# snmpget -v2c -c public 10.50.0.227 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (104027) 0:17:20.27
[root@zbx-60-mysql-ol8 ~]# snmpget -v2c -c public 10.50.0.227 DISMAN-EVENT-MIB::sysUpTimeInstance
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (104555) 0:17:25.55
```

MONITORAMENTO VIA SNMP

MIB E OID

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