

The Zabbix logo, consisting of the word "ZABBIX" in white uppercase letters on a red rectangular background.

**ZABBIX**

LATIN AMERICA

MEETUP  
OFICIAL /2022

BOAS PRÁTICAS DE MONITORAMENTO  
COM ZABBIX

# ZABBIX MEETUP SÃO PAULO

**PRESENCIAL**

Hernandes Martins

# BOAS PRÁTICAS DE MONITORAMENTO COM ZABBIX



**Hernandes Martins**

# Hernandes Martins

- São Paulo – SP
- Atuando com Zabbix desde 2011
- Zabbix Trainer, Consultor e Especialista Zabbix
- Atualmente trabalhando na Radar Payments em Budapest - Hungria
- Colaborador nos canais da Comunidade Zabbix Brasil(Facebook, Telegram, LinkedIn, Youtube)



# O que precisa ser feito?

- Mapear seu negócio dividindo em camadas.

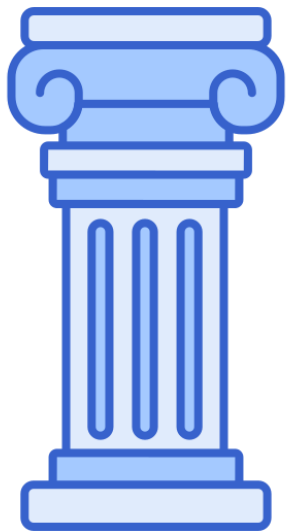
## Camadas

- Estratégico
- Tático
- Operacional

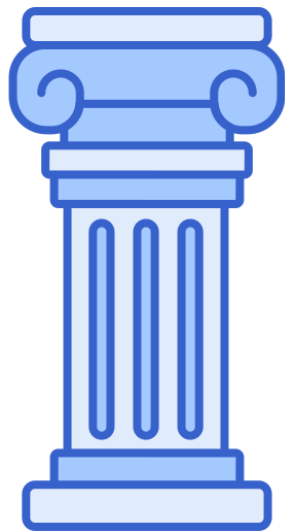
## Decisores, Responsáveis

- ✓ Diretoria, Presidente, CEO,
- ✓ Gerentes
- ✓ Coordenadores, Supervisores, Líder técnico

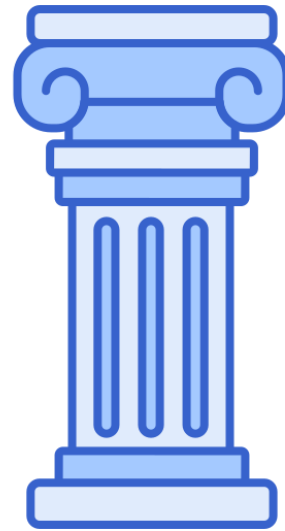
# Os pilares das boas práticas



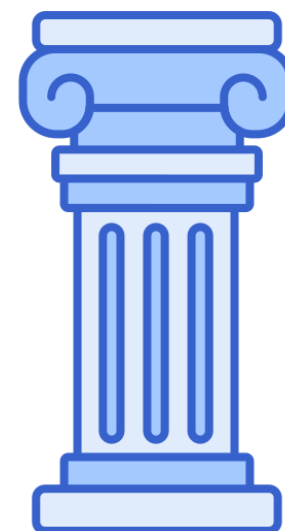
Planejar



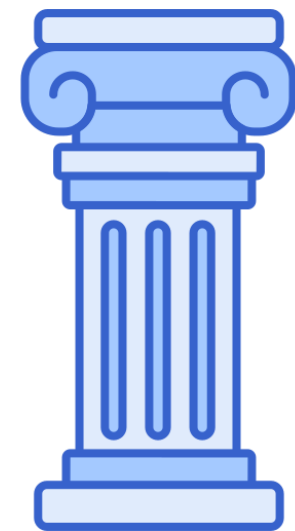
Documentar



Executar



Interagir



Solucionar

### Planejar

- Ao realizar um planejamento é possível entender as etapas para alcançar o objetivo.

- ✓ **Crie seu plano de monitoramento**



Planejar

Seu plano de monitoramento deve responder algumas questões

- ✓ Quais são os objetivos do monitoramento?
- ✓ Quais recursos você vai monitorar?
- ✓ Com que frequência você vai monitorar esses recursos?
- ✓ Quem deve ser notificado quando algo der errado?

### Planejar

- ✓ Faça o monitoramento para gerenciar problemas pequenos antes que eles se tornem grandes.
- ✓ Crie e implemente um plano de monitoramento que colete dados de todas as partes possíveis.
- ✓ Automatize, automatize, automatize!



## Planejar

### ➤ Nomenclaturas

- ✓ Importante criar um padrão de nomes para os dispositivos.
- ✓ Importante segmentar e organizar o ambiente por grupos, áreas, localidades e etc.

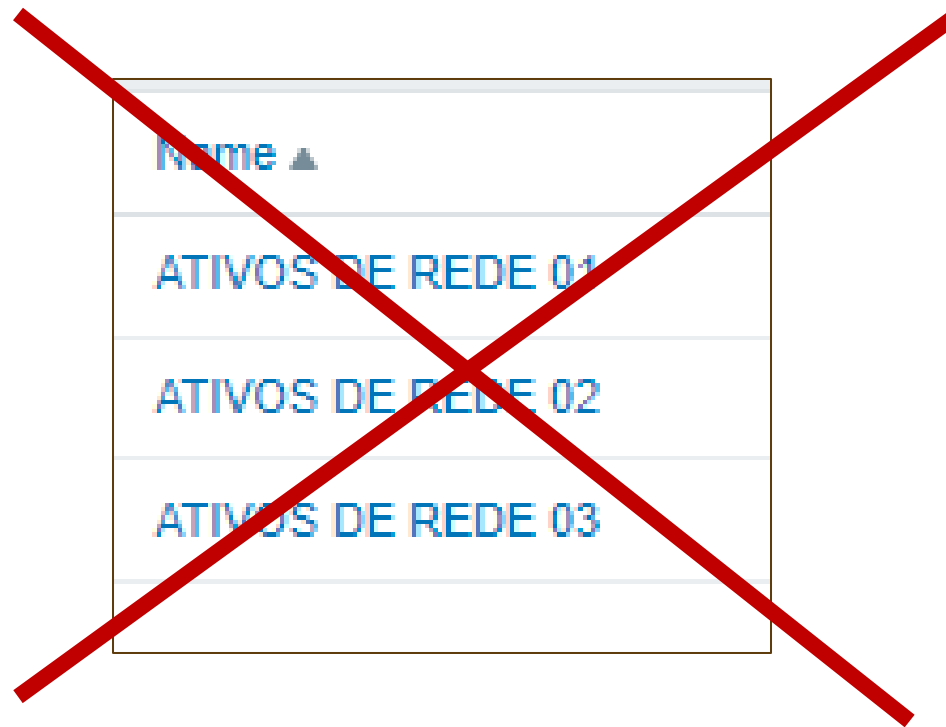
## Planejar

### ➤ Nomenclaturas

✓ Host groups – Não faça isso



Name ▲
CLIENTE_A_FIREWALLS
CLIENTE_A_LINUX
CLIENTE_A_SWITCHES
CLIENTE_A_WINDOWS



Name ▲
ATIVOS DE REDE 01
ATIVOS DE REDE 02
ATIVOS DE REDE 03

## Planejar

## ➤ Nomenclaturas

- ✓ Host groups – Comece pelo básico - Padronize

Modelo	Exemplo
GrupoRaiz	ClienteA
GrupoRaiz/DC	ClienteA/DC
GrupoRaiz/DC/Windows servers	ClienteA/DC/Windows servers
GrupoRaiz/DC/Linux Servers	ClienteA/DC/Linux servers
GrupoRaiz/DC/Applications	ClienteA/DC/Applications

ClienteA
ClienteA/DC
ClienteA/DC/Applications
ClienteA/DC/Linux servers
ClienteA/DC/Windows servers

Simplifique sempre

GrupoRaiz/DC/App

ClienteA/DC/App

ClienteA
ClienteA/DC
ClienteA/DC/App

Hernandes Martins

## Planejar

## ➤ Nomenclaturas

- ✓ Host groups – Crie grupos de categorias

Nome do Grupo	Descrição
Categoria/Routers	Agrupamento de routers
Categoria/Switch	Agrupamento de switches raiz
Categoria/Switch/Dell	Agrupamento de switches Dell
Categoria/Switch/HP	Agrupamento de switches HP
Categoria/Switch/Juniper	Agrupamento de switches Juniper
Categoria/Servidores	Agrupamento de Servidores raiz
Categoria/Servidores/Windows	Agrupamento de Servidores Windows
Categoria/Servidores/Linux	Agrupamento de Servidores Linux
Categoria/Impressoras	Agrupamento de impressoras raiz
Categoria/Impressoras/HP	Agrupamento de impressoras HP
Categoria/Impressoras/EPSON	Agrupamento de impressoras EPSON
Categoria/Impressoras/RICOH	Agrupamento de impressoras RICOH

### Documentar

#### ➤ Por que documentar?

- ✓ Documentar é importante, independente seja ela técnica ou não. A documentação tem como objetivo principal, acompanhar e tornar visível todos os processos e etapas para entrega e continuidade de um projeto.

### Documentar

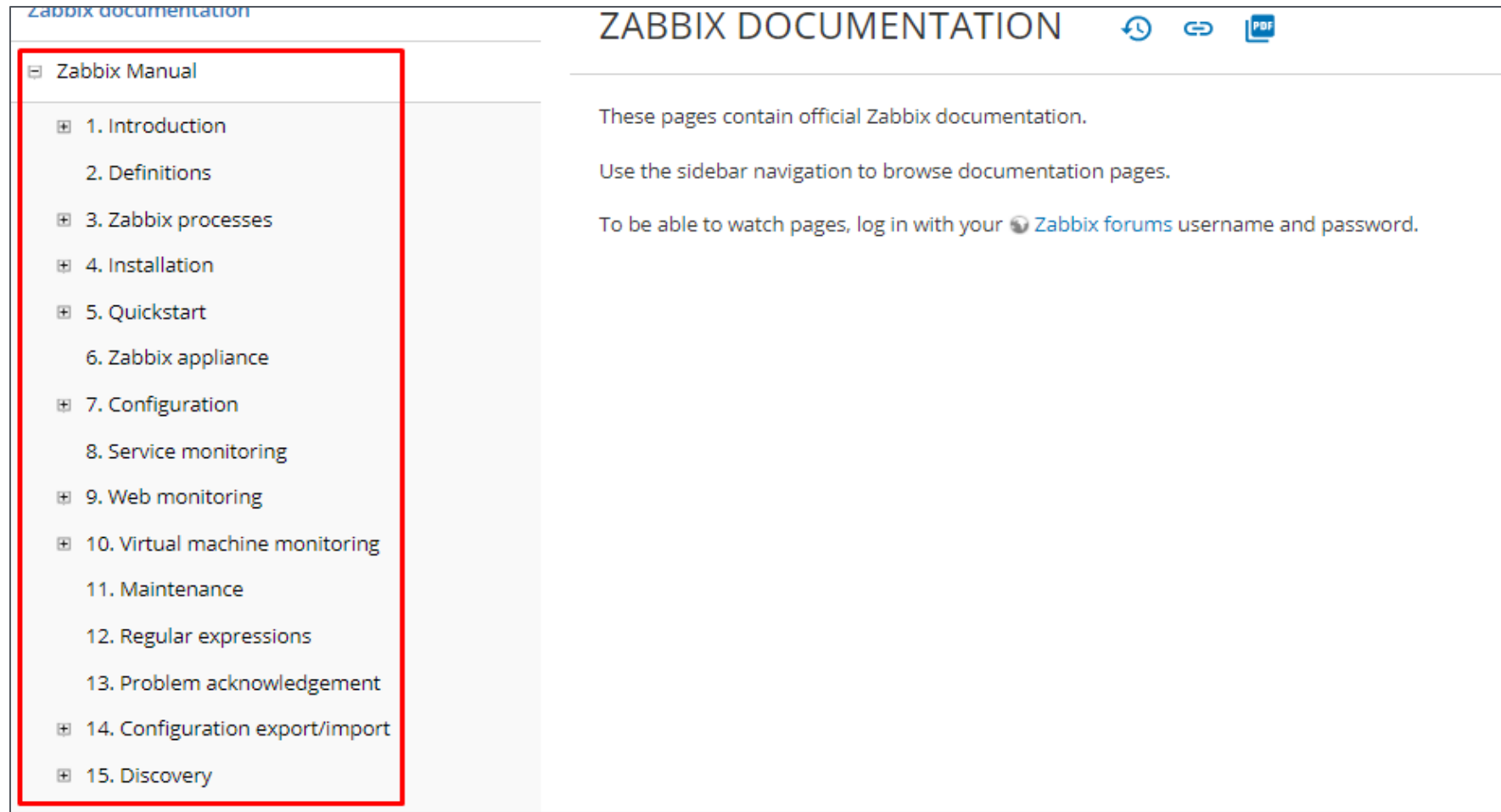
#### ➤ Como documentar?

- ✓ Não existe uma regra ou ferramenta padrão para criação de documentação.
- ✓ A documentação pode ser escrita em um arquivo de texto no Microsoft Word, Wiki, Intranet, Sites com plataformas de documentação, deve ser considerado a praticidade de atualização diária pelo time envolvido na implantação e operação do projeto.

## Documentar

### ➤ Como documentar?

- ✓ Exemplo de documentação em página web.

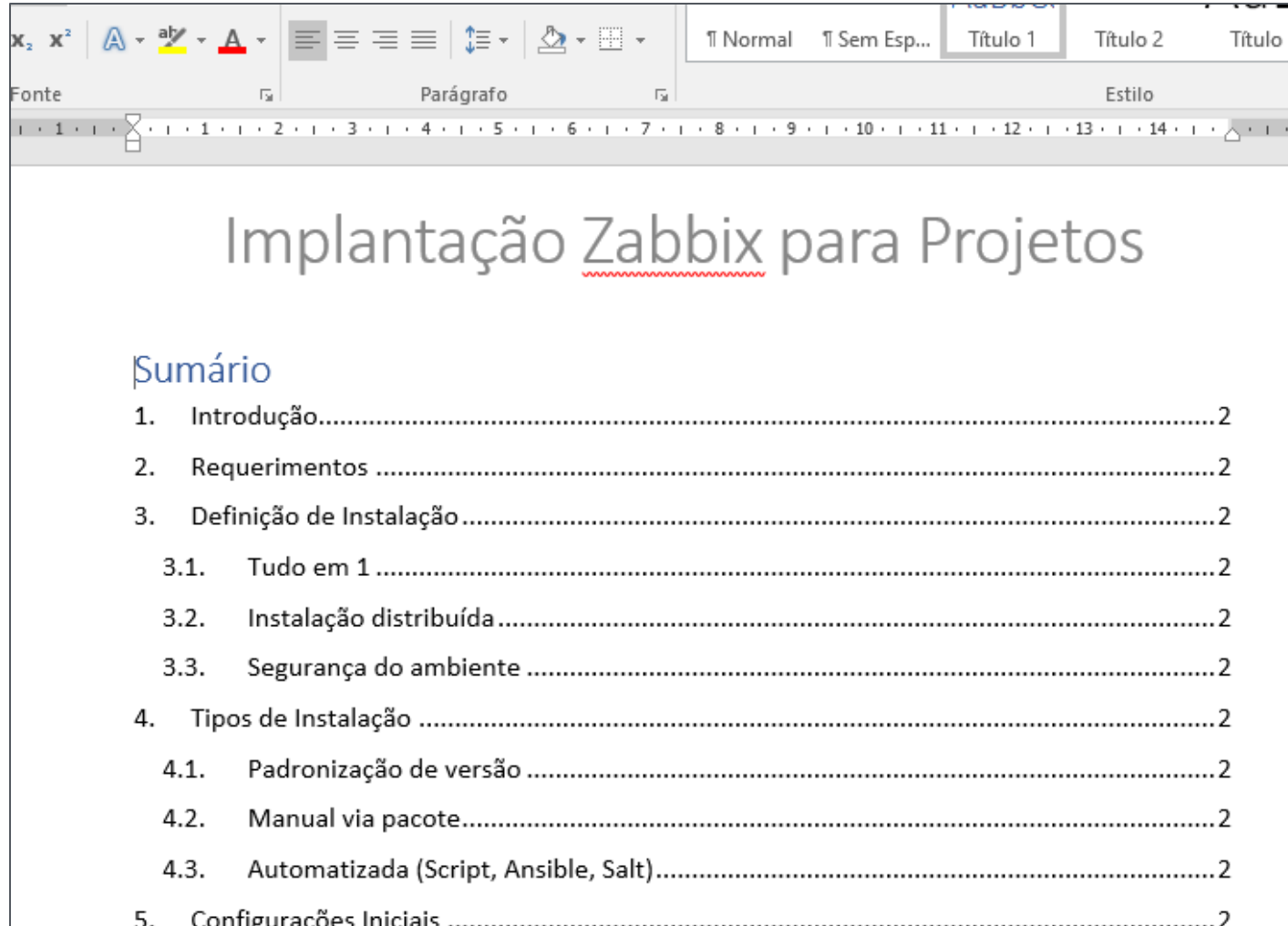




Documentar

➤ Como documentar?

- ✓ Exemplo de documentação em arquivo do Microsoft Word.



Implantação <u>Zabbix</u> para Projetos	
Sumário	
1. Introdução.....	2
2. Requerimentos .....	2
3. Definição de Instalação .....	2
3.1. Tudo em 1 .....	2
3.2. Instalação distribuída .....	2
3.3. Segurança do ambiente .....	2
4. Tipos de Instalação .....	2
4.1. Padronização de versão .....	2
4.2. Manual via pacote.....	2
4.3. Automatizada (Script, Ansible, Salt).....	2
5. Configurações Iniciais .....	2

## ➤ Boas práticas na execução

Executar

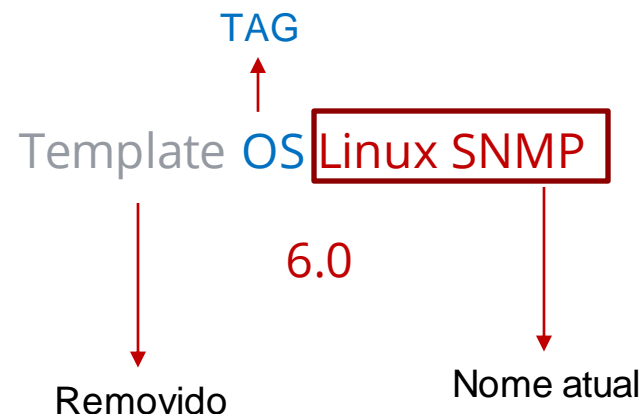
✓ Templates

### Um template deve ser o mais genérico e objetivo possível

- O que permite sua reutilização em diversas camadas (Ex: SNMP device + SNMP switch cisco)
- Um host pode ter vários templates
- Vários templates podem ser associados a um template
- Fique atento, ocorreram mudanças nas nomenclaturas dos templates atuais.

2 templates aplicados para monitoramento completo do host(Switch Cisco)

Template OS Linux SNMP  
5.0



## ➤ Boas práticas na execução

Executar

✓ Itens – Não faça isso

Name ▲	Triggers	Key
ICMP Ping: ICMP loss	Triggers 1	icmppingloss
ICMP Ping: ICMP ping	Triggers 1	icmpping
ICMP Ping: ICMP response time	Triggers 1	icmppingsec
item direto no host		test13
item orfão		teste1
Item sem template		test

- Itens direto no host
- Itens sem template
- Itens orfãos



itens  
sem  
template

itens  
com  
template

## ➤ Boas práticas na execução

Executar

- ✓ Itens – Sempre crie itens dentro do template

Todo item precisa pertencer a um Template

Name ▲	Triggers	Key
<a href="#">ICMP Ping: ICMP loss</a>	<a href="#">Triggers 1</a>	icmppingloss
<a href="#">ICMP Ping: ICMP ping</a>	<a href="#">Triggers 1</a>	icmpping
<a href="#">ICMP Ping: ICMP response time</a>	<a href="#">Triggers 1</a>	icmppingsec
<a href="#">Template Da Hora: item direto no host</a>		test13
<a href="#">Template Da Hora: item orfão</a>		teste1
<a href="#">Template Da Hora: Item sem template</a>		test

Crie Itens e triggers baseados em templates de LLD

## ➤ Boas práticas na execução

### Executar

✓ Itens – Tome cuidado com o tempo de armazenamento

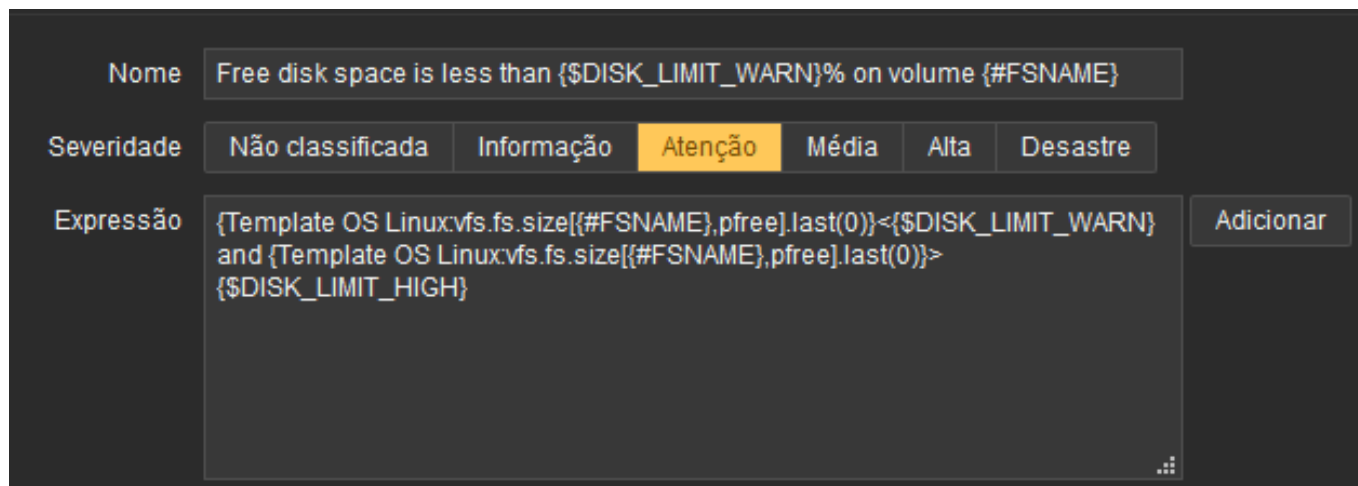
- O Zabbix guarda os dados coletados em dois formatos: History e Trends.
  - O primeiro guarda todos os valores coletados, sem nenhuma sumarização.
  - Os Trends guardam os dados (mínimo, média, máximo e quantidade) sumarizados de hora a hora
- É altamente recomendável guardar o menor histórico o possível para não sobrecarregar o BD com muitos valores históricos.
- No geral, a recomendação é guardar um histórico de 14 dias e médias por até 5 anos. (Atenção: Isso pode variar a cada cliente ou cenário, vai depender da politica de monitoramento)

## ➤ Boas práticas na execução

Executar

- ✓ triggers – sempre use Macros

Macros são variáveis que podem ser configuradas e aplicadas em nível Host, Template ou Global



The screenshot shows the Zabbix trigger configuration interface. The 'Nome' field contains the text 'Free disk space is less than {\$DISK\_LIMIT\_WARN}% on volume {#FSNAME}'. The 'Severidade' field has a dropdown menu with options: 'Não classificada', 'Informação', 'Atenção' (highlighted), 'Média', 'Alta', and 'Desastre'. The 'Expressão' field contains the Zabbix expression: '{Template OS Linux:vfs.fs.size[{#FSNAME},pfree].last(0)}<{\$DISK\_LIMIT\_WARN} and {Template OS Linux:vfs.fs.size[{#FSNAME},pfree].last(0)}>{\$DISK\_LIMIT\_HIGH}'. An 'Adicionar' button is located to the right of the expression field.



The screenshot shows the Zabbix macro configuration interface. It has two tabs: 'Macros de template' and 'Macros herdadas e de template'. The 'Macros de template' tab is active, displaying a table of macros and their values.

Macro	Valor
{CPU_IOWAIT_LIMIT}	= 60
{CPU_STEAL_LIMIT}	= 20
{CPU_USED_AVG}	= 90
{CPU_USED_HIGH}	= 95
{CPU_USED_WARN}	= 80
{DISK_LIMIT_HIGH}	= 5
{DISK_LIMIT_WARN}	= 10

## ➤ Boas práticas na execução

Executar

- ✓ triggers – sempre documente a resolução dos incidentes na descrição da trigger.

- Quem está a frente do monitoramento, nem sempre tem o mesmo conhecimento de quem criou o monitoramento.
- Na configuração da trigger tem campos para remeter a informação sobre como resolver o incidente, pode ser colocado uma URL (exemplo: wiki) ou uma descrição:

URL	<input type="text"/>
Descrição	<div>1) Verificar o status do agent: <code>/etc/init.d/zabbix_agentd status</code>  2) Caso esteja parado somente dar um start. E caso esteja com status de rodando, verificar se há poucos processos, caso tenha poucos processos, os mesmos devem estar travados e será necessário reiniciar o agent.</div>



## ➤ Boas práticas

Executar

✓ triggers

trigger.

- O que está chegando nas

<https://support.zabbix.com/browse/ZBX>

### Current problems

Time ▼	Info	Host	Problem • Severity
07:53:26		Zabbix server	Zabbix agent is not

\* Expression

```
max(/Zabbix server/zabbix[host,agent,available],  
{ $AGENT.TIMEOUT })=0
```

Add

Expression constructor

OK event generation

Expression

Recovery expression

None

PROBLEM event generation mode

Single

Multiple

OK event closes

All problems

All problems if tag values match

Allow manual close



Menu entry name ?

KB Article

Menu entry URL

<https://oicts.atlassian.net/wiki/spaces/IN/pages/1734567/{HOSTID}>

Description

For passive only agents, host availability is used with { \$AGENT.TIMEOUT } as time threshold.

Enabled



Update

Clone

Delete

Cancel

➤ **Boas práticas na execução**

- Sempre observe seus itens não suportados
- Sempre revise seus intervalos de coleta de dados
- Mantenha seus agentes atualizados(Automatize, use orquestração (ansible,puppet,saltstack).
- Fique de olho nos problemas com mais de 20d (Use período de manutenção)
- Use proxy

### Interagir

- A ferramenta de monitoramento deve interagir com outros tipos de ferramentas e tecnologias:
  - ✓ Abertura de Tickets (OTRS, GLPI, Webhooks diversos)
  - ✓ Dashboards (Zabbix + Grafana + Desenvolvimento)
  - ✓ (Ocs Inventory)
  - ✓ Relatórios, Hardware (Arduíno, IOT e Automações)

### Solucionar

- Solucionar é dos fatores decisivos na escolha de uma ferramenta de monitoração.
  - ✓ Deve ser pensando, que em caso de falhas, é possível realizar algo de forma automatizada para restabelecer o serviço.
  - ✓ Validar a possibilidade utilizar scripts e ou adicionar protocolos diferenciados(Ex: Modbus)

# Hernandes Martins

Facebook: @mrhernandesmartins

Twiter: @SuperHernandes

Linkedin: Hernandez Martins

Youtube: HernandezMartins



# OBRIGADO