TOP 20 PROCESS WINDOWS

ZABBIX

Sumário

TOP 20 Process Windows 4
1. Apresentação 5
Requisitos & Template 6
2. Preparação do Host 7
3. Itens 7
4. Triggers 7
5. Macros 7
Instalação do Agente Customizado 8
6. Agente Zabbix Top 20 Process 9
7. Associação de Templates 9
Configuração Manual 10
8. Preparando o Host 11
9. Procedimentos 11
10. Validação do Script DiscoveryProcess.ps1 12
11. Template 13
Dados e Gráficos 14
12. Dados Recentes 15

Descrição	Autor	Revisão
Projeto Monitoramento de Processo do Windows	Idealizador: Magno Monte Cerqueira	V.1.0
DiscoveryProcess.ps1 com passagem de parâmetros para coleta do tempo de CPU por um processo. Memória utilizada pelo processo	Danilo Barros	V.1.2
Item.cpu.ps1 coleta a utilização de CPU por processo em porcentagem.	Magno Monte Cerqueira	V.1.0
zabbixAgent-4.0.1_installer_TOP20_Process_Windows.exe Agente customizado com toda a integração do Userparameter e scripts Powershell	Danilo Barros	V.1.0.7

TOP 20 Process Windows

1. Apresentação

O presente documento tem por objetivo apresentar todas as etapas técnicas para implantação do monitoramento de processos do Windows utilizando scripts em Powershell V.5.0, LLD e a função do Userparameter do agente Zabbix.

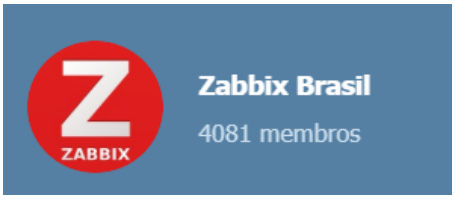
Projeto idealizado na comunidade Zabbix Brasil no Telegram pelo usuário Magno Monte Cerqueira e Danilo Barros.

Inicialmente existiam dois protótipos em desenvolvimento destinado a comunidade, no decorrer das atividades surgiu a necessidade da junção dos dois modelos em um único script com passagens de parâmetros e com coletas do tipo top/down para os primeiros 20 processos com maior tempo de CPU (Do maior tempo de CPU para o menor).

Créditos Desenvolvedores:

Danilo Barros de Medeiros
Zabbix Certified Specialist
Zabbix Certified Professional
Danilo@provtel.com.br
www.provtel.com.br

Magno Monte Cerqueira
Instrutor Treinamentos Zabbix
Apoiador da Comunidade Zabbix Brasil
magno.cerqueira@2mti.com.br
https://treinamentos.2mti.com.br



Links de acesso a comunidade Zabbix Brasil Telegram:
https://t.me/ZabbixBrasil
@ZabbixBrasil

Requisitos & Template

2. Preparação do Host

Para realizar o monitoramento via Powershell é necessário a liberação para execução de scripts. A política de execução faz parte da estratégia de segurança do PowerShell. Ele determina se você pode carregar arquivos de configuração (incluindo seu perfil do PowerShell) para executar scripts. O cmdlet **Set-ExecutionPolicy** altera a preferência do usuário para a diretiva de execução do PowerShell.

- Abra o Powershell como Administrador e execute o comando Set-ExecutionPolicy Unrestricted e confirme.
- Caso já tenha feito o procedimento acima no Host, desconsidere e pule para o próximo requerimento.

3. Itens

Nome Template: *Template_Monitoramento_TOP20_Process_Windows.xml*

- LLD discovery.processos.windows
- LLD Consumo de CPU %
- LLD Consumo de Memory
- LLD Tempo Utilização CPU

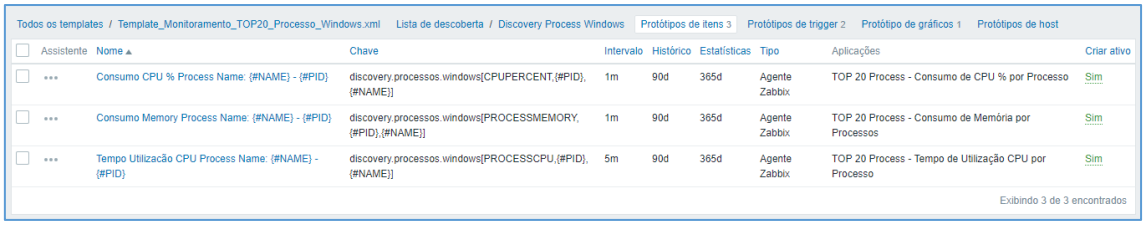


Figura 1 - Protótipos de itens LLD

4. Triggers

- Consumo de CPU pelo Processo {#NAME} está acima de 90% por mais de 10min no servidor {HOST.NAME}
- Consumo de memória pelo Processo {#NAME} está acima de 1GB por mais de 10min no servidor {HOST.NAME}

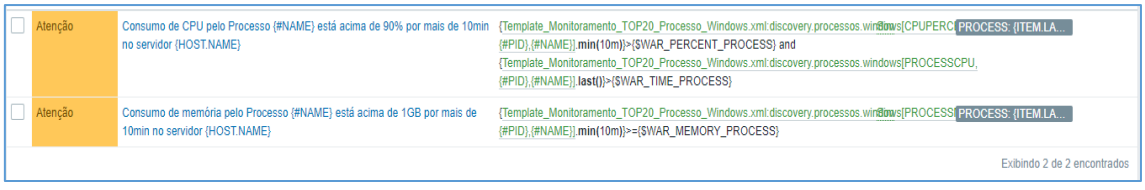


Figura 2 - Protótipos de triggers

5. Macros

- {$WAR_MEMORY_PROCESS} = 1G
- {$WAR_PERCENT_PROCESS} = 90
- {$WAR_TIME_PROCESS} = 600

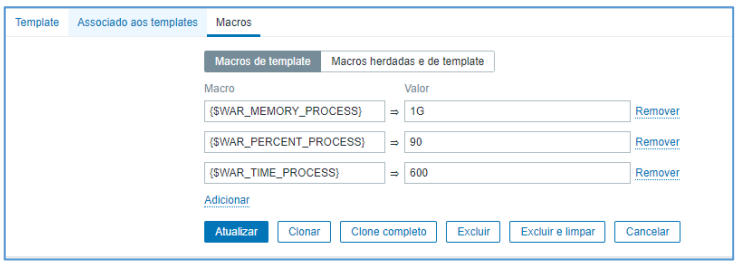


Figura 3 - Macros templates

Instalação do Agente Customizado

6. Agente Zabbix Top 20 Process

- Agente disponibilizado junto com pacote de instalação
- Execução do agente (*zabbixAgent-4.0.1_installer_TOP20_Process_Windows.exe*)

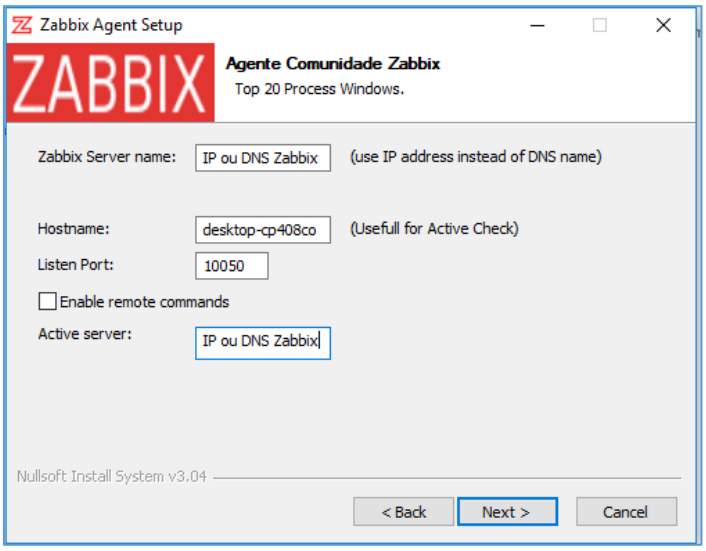


Figura 4 - Instalação do Agente Zabbix TOP 20 Process

Informativos:

- O agente customizado já possui todas as configurações referente a cópia do script para o diretório "C:\Program Files\Zabbix Agent"
- Configuração do arquivo "zabbix_agentd.conf" com a inserção de parâmetros.
- **Linha 280** do arquivo Zabbix_agentd.conf

  UserParameter=discovery.processos.windows[*],powershell.exe -noprofile -executionpolicy bypass -File "C:\Program Files\Zabbix Agent\DiscoveryProcess.ps1" $1 $2

7. Associação de Templates

Associar o *Template_Monitoramento_TOP20_Processo_Windows.xml* ao host Windows a ser monitorado.

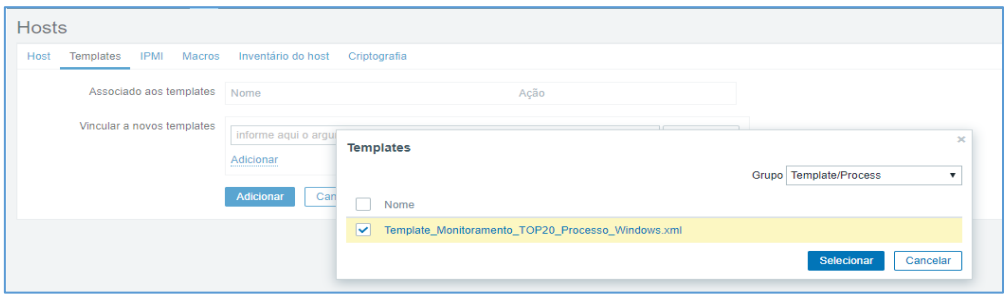


Figura 5 - Associar template ao Host

Configuração Manual

8. Preparando o Host

Para habilitar o monitoramento Top 20 Process em ambientes em produção onde não é permitido a instalação de um novo agente, ou por processos internos, ou por um possível impacto nas coletas de dados ou então por falta de uma janela de manutenção esse item informa os procedimentos para ativar o monitoramento no Host para esses possíveis cenários.

TOP 20 PROCESS.zip

Extrair os seguintes arquivos:

- discovery.Process.conf
- DiscoveryProcess.ps1
- Template_Monitoramento_TOP20_Process_Windows.xml

9. Procedimentos

- Copie o arquivo DiscoveryProcess.ps1 no diretório de sua escolha.
- Copie o arquivo discovery.Process.conf no diretório de sua escolha.
- Reinicie o Zabbix Agent no Host.
-

Segue o exemplo seguir: C:\Program Files\Zabbix Agent

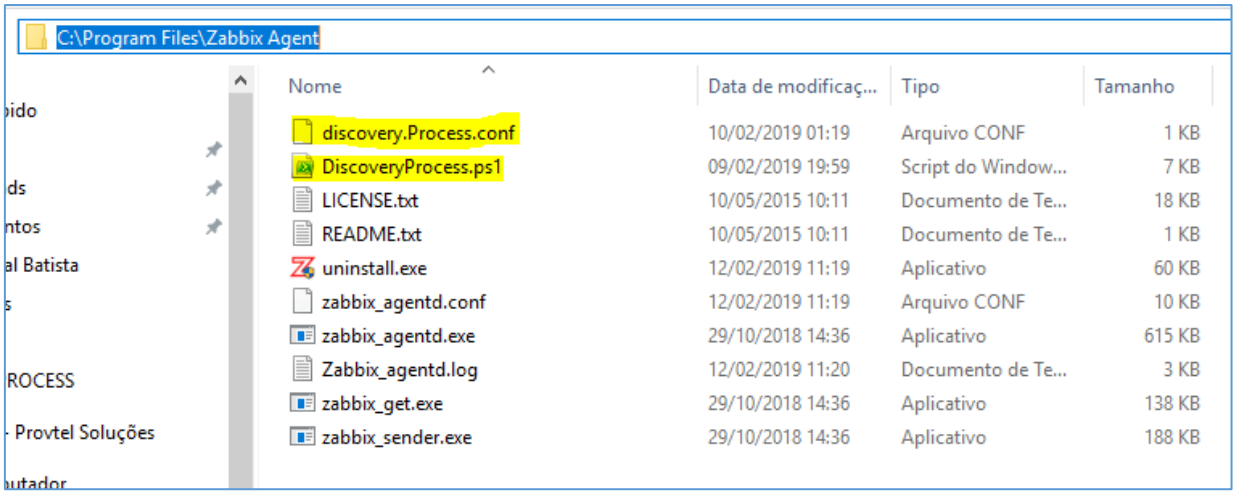


Figura 6 - Cópia dos arquivos de configuração para diretório Zabbix Agent

10. Validação do Script DiscoveryProcess.ps1

Abra o Powershell e navegue até a pasta do script onde foi realizada a cópia: Segue o exemplo:

```
PS C:\Program Files\Zabbix Agent> .\DiscoveryProcess.ps1 DISCOVERY
{
 "data":[

{ "{#NAME}":"chrome","{#PID}":"1012"},
{ "{#NAME}":"chrome","{#PID}":"1380"},
{ "{#NAME}":"chrome","{#PID}":"1908"},
{ "{#NAME}":"chrome","{#PID}":"4176"},
{ "{#NAME}":"chrome","{#PID}":"8604"},
{ "{#NAME}":"chrome","{#PID}":"8900"},
{ "{#NAME}":"chrome","{#PID}":"9164"},
{ "{#NAME}":"chrome","{#PID}":"9620"},
{ "{#NAME}":"chrome","{#PID}":"9892"},
{ "{#NAME}":"chrome","{#PID}":"10572"},
{ "{#NAME}":"core","{#PID}":"6976"},
{ "{#NAME}":"ctfmon","{#PID}":"1152"},
{ "{#NAME}":"EXCEL","{#PID}":"6596"},
{ "{#NAME}":"explorer","{#PID}":"7316"},
{ "{#NAME}":"MicrosoftEdge","{#PID}":"6420"},
{ "{#NAME}":"MicrosoftPdfReader","{#PID}":"7264"},
{ "{#NAME}":"OneDrive","{#PID}":"10680"},
{ "{#NAME}":"SearchUI","{#PID}":"8544"},
{ "{#NAME}":"svchost","{#PID}":"2968"},
{ "{#NAME}":"WINWORD","{#PID}":"10844"},
{ "{#NAME}":"filtro","{#PID}":"00000"}

 ]
}

PS C:\Program Files\Zabbix Agent> |
```

Figura 7 - Execução do Discovery dos processos Windows

Selecione um PID do resultado do Discovery e execute os parâmetros abaixo.

```
PS C:\Program Files\Zabbix Agent> .\DiscoveryProcess.ps1 PROCESSCPU 10844
1814
```

Figura 8 - Coleta do tempo de CPu do Processo

```
PS C:\Program Files\Zabbix Agent> .\DiscoveryProcess.ps1  PROCESSMEMORY 10844
199090176
```

Figura 9- Coleta da utilização da memória pelo processo

```
PS C:\Program Files\Zabbix Agent> .\DiscoveryProcess.ps1  CPUPERCENT 10844
0
```

Figura 10 - Utilização da CPU em %

11. Template

- Importe o Template - *Template_Monitoramento_TOP20_Processo_Windows.xml*
- Associe o Template ao Host a ser monitorado.
- Aguarde a coleta dos dados.

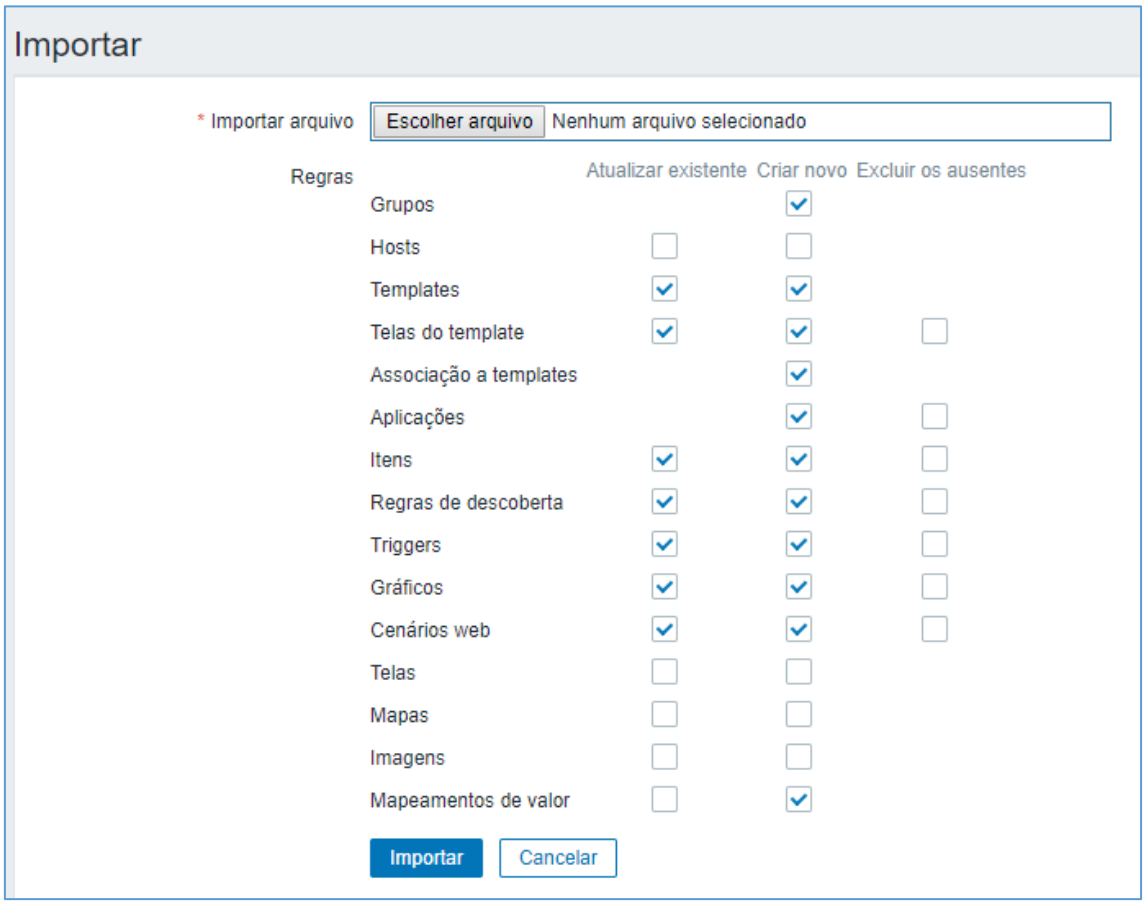
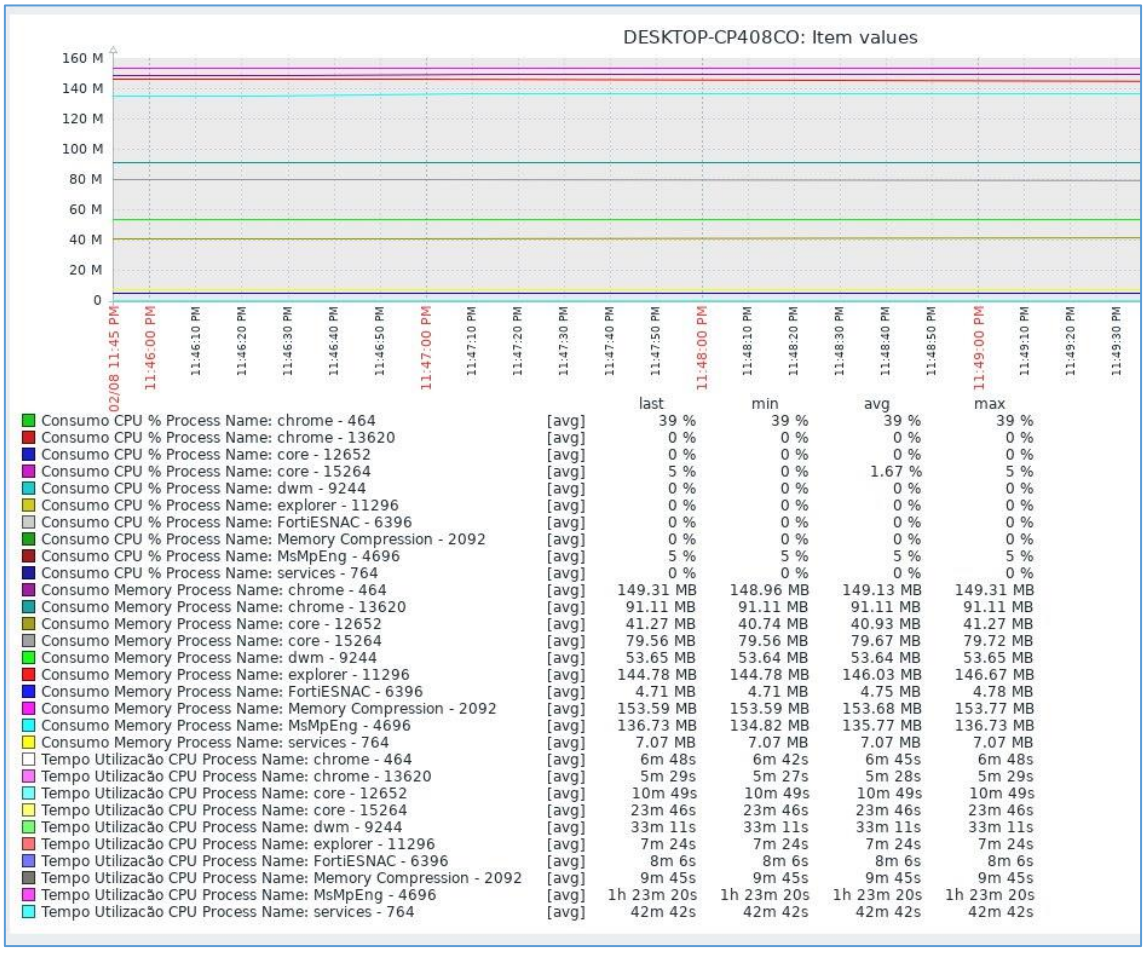


Figura 11 - Importar template

Dados e Gráficos

12. Dados Recentes



		last	min	avg	max
Consumo CPU % Process Name: chrome - 464	[avg]	39 %	39 %	39 %	39 %
Consumo CPU % Process Name: chrome - 13620	[avg]	0 %	0 %	0 %	0 %
Consumo CPU % Process Name: core - 12652	[avg]	0 %	0 %	0 %	0 %
Consumo CPU % Process Name: core - 15264	[avg]	5 %	0 %	1.67 %	5 %
Consumo CPU % Process Name: dwm - 9244	[avg]	0 %	0 %	0 %	0 %
Consumo CPU % Process Name: explorer - 11296	[avg]	0 %	0 %	0 %	0 %
Consumo CPU % Process Name: FortiESNAC - 6396	[avg]	0 %	0 %	0 %	0 %
Consumo CPU % Process Name: Memory Compression - 2092	[avg]	0 %	0 %	0 %	0 %
Consumo CPU % Process Name: MsMpEng - 4696	[avg]	5 %	5 %	5 %	5 %
Consumo CPU % Process Name: services - 764	[avg]	0 %	0 %	0 %	0 %
Consumo Memory Process Name: chrome - 464	[avg]	149.31 MB	148.96 MB	149.13 MB	149.31 MB
Consumo Memory Process Name: chrome - 13620	[avg]	91.11 MB	91.11 MB	91.11 MB	91.11 MB
Consumo Memory Process Name: core - 12652	[avg]	41.27 MB	40.74 MB	40.93 MB	41.27 MB
Consumo Memory Process Name: core - 15264	[avg]	79.56 MB	79.56 MB	79.67 MB	79.72 MB
Consumo Memory Process Name: dwm - 9244	[avg]	53.65 MB	53.64 MB	53.64 MB	53.65 MB
Consumo Memory Process Name: explorer - 11296	[avg]	144.78 MB	144.78 MB	146.03 MB	146.67 MB
Consumo Memory Process Name: FortiESNAC - 6396	[avg]	4.71 MB	4.71 MB	4.75 MB	4.78 MB
Consumo Memory Process Name: Memory Compression - 2092	[avg]	153.59 MB	153.59 MB	153.68 MB	153.77 MB
Consumo Memory Process Name: MsMpEng - 4696	[avg]	136.73 MB	134.82 MB	135.77 MB	136.73 MB
Consumo Memory Process Name: services - 764	[avg]	7.07 MB	7.07 MB	7.07 MB	7.07 MB
Tempo Utilização CPU Process Name: chrome - 464	[avg]	6m 48s	6m 42s	6m 45s	6m 48s
Tempo Utilização CPU Process Name: chrome - 13620	[avg]	5m 29s	5m 27s	5m 28s	5m 29s
Tempo Utilização CPU Process Name: core - 12652	[avg]	10m 49s	10m 49s	10m 49s	10m 49s
Tempo Utilização CPU Process Name: core - 15264	[avg]	23m 46s	23m 46s	23m 46s	23m 46s
Tempo Utilização CPU Process Name: dwm - 9244	[avg]	33m 11s	33m 11s	33m 11s	33m 11s
Tempo Utilização CPU Process Name: explorer - 11296	[avg]	7m 24s	7m 24s	7m 24s	7m 24s
Tempo Utilização CPU Process Name: FortiESNAC - 6396	[avg]	8m 6s	8m 6s	8m 6s	8m 6s
Tempo Utilização CPU Process Name: Memory Compression - 2092	[avg]	9m 45s	9m 45s	9m 45s	9m 45s
Tempo Utilização CPU Process Name: MsMpEng - 4696	[avg]	1h 23m 20s	1h 23m 20s	1h 23m 20s	1h 23m 20s
Tempo Utilização CPU Process Name: services - 764	[avg]	42m 42s	42m 42s	42m 42s	42m 42s

Figura 12 - Gráficos simples

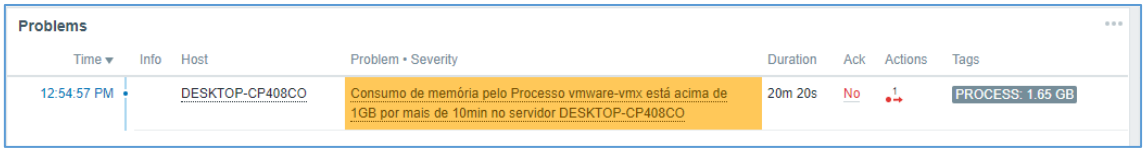


Figura 13 - Trigger Process