Introdução ao Sistema de Monitoramento Zabbix

Fernando B. de Souza, Evandro C. Vilas Boas, Francisco A. S. do Carmo
Laboratório de Cyber Segurança e Internet das Coisas (CS&I Lab.), Instituto Nacional de Telecomunicações - Inatel
fernandobatista@get.inatel.br, evandro.cesar@inatel.br, francisco.assis@inatel.br

***Abstract*—This work describes the development of Zabbix monitoring system experiments. It demonstrates the system's implementation in a virtualized environment, monitoring server and the information synchronization agent configurations. It addresses relevant aspects of network monitoring and management. This brief tutorial represents a summary of an experiment prepared for Inatel's (National Institute of Telecommunications) Network Management and Cybersecurity Laboratory.**

***Index Terms*—Cyber security, network management, network monitoring, Zabbix.**

***Resumo*—Esse trabalho descreve o desenvolvimento de experimentos práticos utilizando o sistema de monitoramento Zabbix. Demonstra-se a implementação do sistema em ambiente virtualizado, a configuração do servidor de monitoramento e do agente de sincronismo de informações. Abordam-se aspectos relevantes sobre o monitoramento e gerência de redes. Esse breve tutorial representa um resumo de um caderno elaborado para o Laboratório de gerência de redes e segurança cibernética do Inatel (Instituto Nacional de Telecomunicações).**

***Palavras chave*—Gerência de redes, monitoramento de redes, segurança cibernética, Zabbix.**

I. Introdução

O conceito de monitoramento e gerenciamento de dispositivos de redes é inerente à disponibilidade, segurança e estabilidade [1, 2]. O gerenciamento e monitoramento de ativos de redes é de extrema importância para centros de controle de redes na manutenção e identificação de possíveis incidentes de segurança [3, 4]. A indisponibilidade de um sistema ou rede de telecomunicações é uma falha de segurança, assim como a instabilidade. Por isso, o monitoramento é abordado como uma técnica capaz de auxiliar na mitigação de riscos. Existem inúmeras ferramentas e sistemas capazes de realizar o monitoramento e a gerência das redes. Citam-se o Zabibix, Cacti, Nagios, PRTG Network Monitor e Munin como as principais.

Nesse trabalho, explora-se o sistema de monitoramento Zabbix para a elaboração de um experimento prático [1, 5]. Selecionou-se essa ferramenta entre as supracitadas por permitir integrar a tomada de decisões básicas por meio da aplicação de controles de inteligência artificial e aprendizado de máquinas em relação ao comportamento de conexão de rede, consumo de memória, processamento e armazenamento. Alinhando-se aos objetivos de trabalhos futuro. O Zabbix é um *software* de código aberto para uso acadêmico e comunitário. Apresenta como principais características o uso de scripts personalizados, monitoramento em tempo real, customização e fácil integração com bancos de dados.

Para desenvolver o experimento, utiliza-se uma imagem de sistema já concebida, conhecida comumente como *Open Virtual Applications* (OVA). Configura-se o sistema Zabbix para operação em uma arquitetura cliente-servidor. Dessa forma, sincronizam-se em tempo quase real os reportes de situação de clientes com o servidor que coleta, analisa, processa e exibe os resultados de forma gráfica para os centros de controle de redes. Estruturou-se o trabalho em cinco seções. Na Seção II, demonstram-se as configurações iniciais do ambiente para desenvolvimento do experimento. Discute-se a preparação do cliente Zabbix na Seção III. Executa-se o monitoramento Zabbix e avaliam-se alguns resultados na Seção IV. Na Seção V, abordam-se os principais comentários e conclusões, assim como trabalhos futuros.

II. Configurações Inicias do Ambiente

Nessa seção, dispõem-se os passos para as configurações iniciais do ambiente empregado durante o experimento. Utilizou-se ambientes com as seguintes configurações:

- Sistema Operacional VWMare Vsphere ESXi versão 7.0;
- Virtual Apliance do Sistema Zabbix (arquivo OVA);

Instalou-se o sistema operacional em um servidor Dell Power Edge R430 Series e importou-se o arquivo OVA no ambiente do sistema operacional, resultando em uma máquina virtual que já possui o sistema Zabbix instalado. Pode-se instalar o sistema em máquinas com sistemas operacionais Linux ou MS Windows com base em repositórios públicos disponíveis no Github.com. Não se recomenda essa prática. Encontra-se a distribuição oficial do Zabbix em (https://www.zabbix.com/cloudimages), sendo empregada nesse trabalho. Após instalar o arquivo OVA, pode-se inicializar a máquina virtual e acessá-la via navegador web por meio do respectivo endereço IP. Na Figura 1, tem-se a tela de *login* do sistema Zabbix.

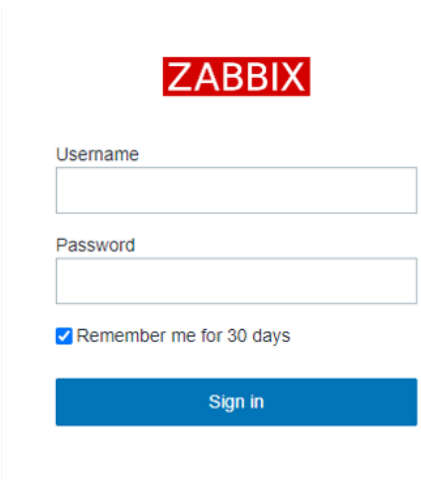

Fig. 1. Tela de *login* do Zabbix.

Após o *login*, tem-se acesso à tela de configuração do sistema, como visto na Figura 2. Nessa tela, verificam-se alguns itens importantes como o *status* do serviço Zabbix onde o campo "Valor" deve estar indicando "Sim"e o campo "Detalhes", o endereço da porta de conexão padrão dos agentes Zabbix. A informação contida no segundo campo é importante para a tarefa de configuração do agente de conexão, assim como o endereço de IP do servidor Zabbix.

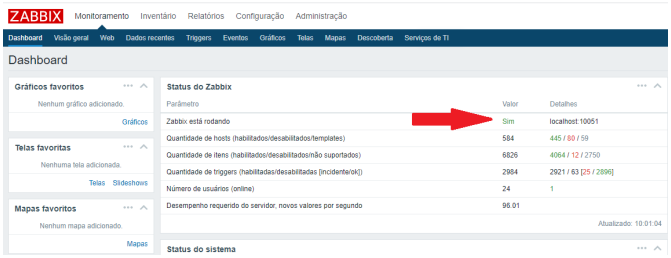

Fig. 2. Tela inicial do Zabbix.

Caso o campo "Valor" indique a mensagem "Não", deve-se iniciar o serviço por meio de comandos específicos no prompt de comando ou shell do servidor:

- service zabbix-server start
- /etc/init.d/zabbix-server start ou a sequência abaixo
- service zabbix-server restart
- service zabbix-server stop
- service zabbix-server start
- service zabbix-server status

Recomenda-se incluir todos os comandos listados, pois algumas distribuições de OVA podem ser distribuições Linux diferentes. Logo, mitiga-se o risco de um comando não estar adequado à distribuição.

III. Instalação do Cliente Zabbix

Realizou-se a instalação de cliente Zabbix em um dispositivo com sistema operacional MS Windows 10 Pro. Sincronizou-se esse dispositivo ao servidor Zabbix, que possui um *template* associado com os devidos controles ativos no servidor. Para instalar o cliente, acessa-se o sistema operacional MS Windows 10 Pro. Na sequência, abre-se o MS Windows Explorer e navega-se até a pasta "zabbix"no disco local C:, onde estão os arquivos de configuração conforme apresentado na Figura 3.

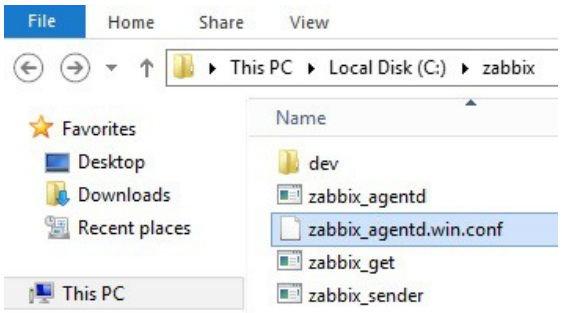

Fig. 3. Arquivos na pasta zabbix.

Em seguida, edita-se o arquivo "zabbix-agentd.win.conf" com um editor de texto. No arquivo, realizam-se as seguintes alterações:

- Server = IP do Servidor Zabbix;
- ListenIP = IP do computador a ser monitorado;
- ServerActive = IP od Servidor Zabbix;
- Hostname = zabbix-server (Servidor Zabbix).

Após efetuar as alterações e salvá-las, acessa-se o prompt de comando da máquina com privilégios de administrador e executa-se o comando na Figura 4.

```
c:\zabbix\zabbix_agentd.exe --config c:\zabbix\zabbix_agentd.win.conf --install
```

Fig. 4. Execução de comando zabbix no Prompt.

Se a execução ocorrer corretamente, visualizam-se as mensagens na Figura 5. Caso o comando retorne resultados diferentes, deve-se revisar as configurações do arquivo e repetir a tarefa de execução.

```
zabbix_agentd.exe [4508]: service [Zabbix Agent] installed successfully
zabbix_agentd.exe [4508]: event source [Zabbix Agent] installed successfully
```

Fig. 5. Resposta ao comando executado na Figura 4.

Em seguida, inicia-se o serviço Zabbix por meio da interface de gestão de tarefas e serviços do MS Windows 10 Pro. Na Figura 6, indica-se essa tarefa.

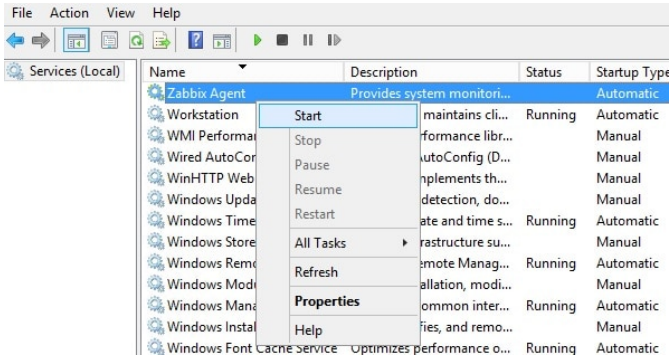

Fig. 6. Iniciando o serviço Zabbix Agent no MS Windows.

Após instalar o Zabbix Cliente e inicializá-lo no sistema operacional MS Windows 10 Pro, deve-se garantir que existam regras de *firewall* para a correta comunicação entre o cliente e o servidor Zabbix. Portanto, deve-se avaliar se a porta de comunicação do Zabbix está aberta no dispositivo, pois é por meio dela que ocorre a comunicação. Caso seja necessário, cria-se regras de entrada e saída no *firewall* do dispositivo. Para saber como criar essa regra, recomenda-se acessar o endereço eletrônico (https://docs.microsoft.com/pt-br/windows/security/threat-protection/windows-firewall/create-an-inbound-program-or-service-rule).

IV. Ativando o Monitoramento no Zabbix

Para realizar o monitoramento do cliente criado na Seção III, deve-se incluí-lo no servidor Zabbix. Na interface de administração do servidor Zabbix, acessa-se a guia "Configuração" e na sequência o item "Host", conforme indicado na Figura 7.

Ao clicar em "Host", seleciona-se "Criar Host"no canto superior direito da tela do Zabbix para acessar a janela de configuração de cliente, exibida na Figura 8. Configuram-se os itens descritos abaixo:

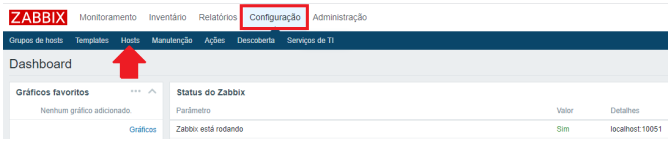

Fig. 7. Acessando a guia ”Configuração”.

- Nome do Host = é propriamente o nome de sistema do dispositivo;
- Nome visível = é o nome que será exibido na interface do Zabbix;
- Novo grupo = para o caso de grupos distintos (ex: Servidores FTP);
- Endereço IP = o endereço do dispositivo a ser monitorado;
- Porta = a porta de conexão do Agente Zabbix;
- Ativo = se marcado, inicia o monitoramento logo após a adição do *host*.

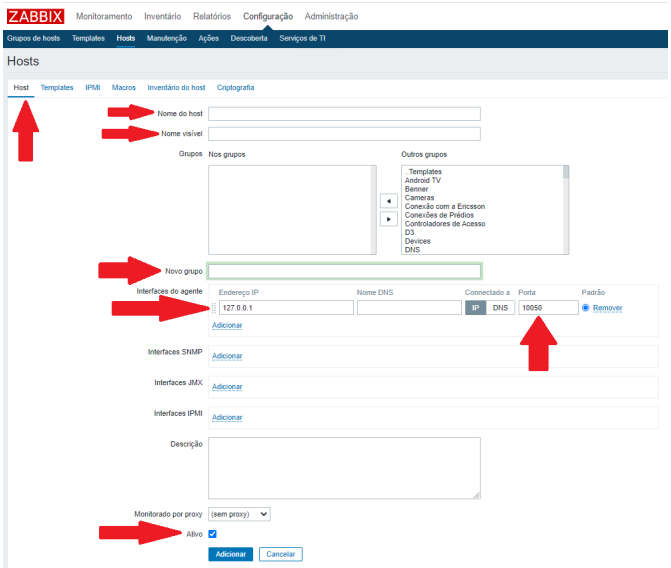

Fig. 8. Itens de configuração na adição de um cliente ao servidor Zabbix.

Ao finalizar as configurações, confirma-se a inclusão do cliente em “Adicionar”. Dessa forma, adicionou-se o dispositivo MS Windows 10 Pro ao servidor Zabbix. Em seguida, deve-se definir o parâmetro de monitoramento desse cliente. Para isso, acessa-se o item “Template” em “Hosts”, que exibe a tela na Figura 9. O sistema de monitoramento Zabbix possui em seu pacote de instalação uma série de *templates* para associação aos diversos tipos de dispositivos e sistemas operacionais [5]. Além disso, pode-se importar para o sistema alguns tipos de *templates* relacionados à dispositivos de interconexão de redes e também dispositivos de segurança, vigilância e controle de acesso. Para esse experimento, seleciona-se o *template* relacionado ao cliente MS Windows 10 Pro por meio da lista, cuja exibição habilita-se em “Selecionar”.

Na sequência, vincula-se o *template* selecionado ao cliente por meio da função “Atualizar”, conforme visto na Figura 10.

Essa ação exibe a tela vista na Figura 11, na qual visualiza-se o dispositivo incluso no servidor Zabbix. Deve-se atentar para os campos nome do *host*, interface e *status*. Nesse momento, todos os itens relacionados ao *template* estão disponíveis para,

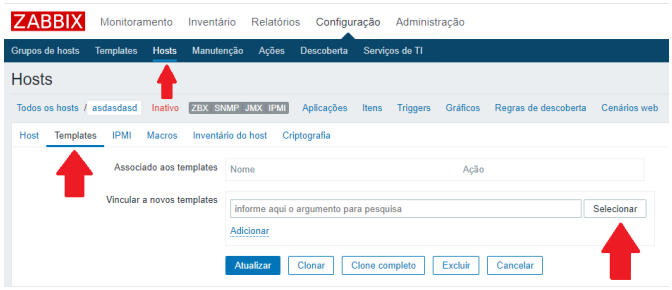

Fig. 9. Atribuindo um template ao ”Host”.

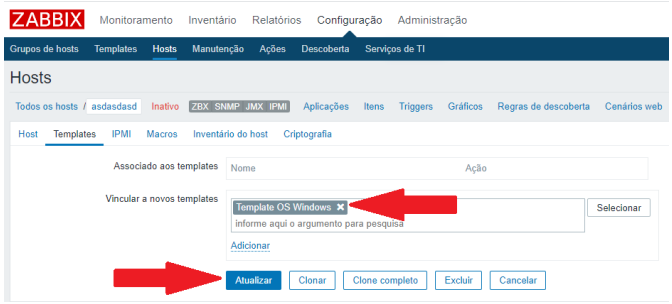

Fig. 10. Vincular ”Templates”.

por exemplo, geração de gráficos de desempenho. Esses itens referem-se ao consumo de processamento, memória, armazenamento, conexão de rede, etc. A ferramenta dispõe os gráficos em *dashboards*, com a possibilidade de integrá-los a outros sistemas de monitoramento e alerta que se comunicam com o Zabbix.

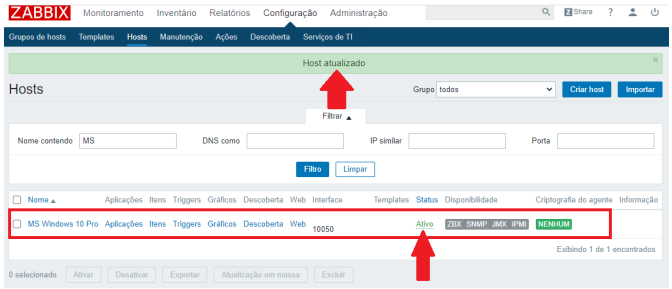

Fig. 11. Dispositivo com informações atualizadas.

Para gerar um gráfico em tempo real do dispositivo MS Windows 10 Pro, clica-se sobre ele e seleciona-se a guia“Gráficos”, conforme demostrado na Figura 12.

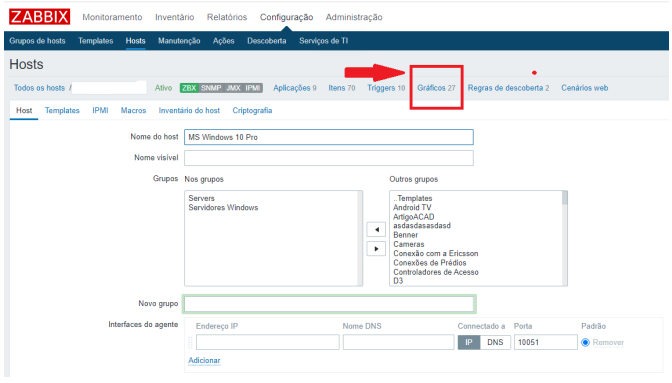

Fig. 12. Criação de um gráfico.

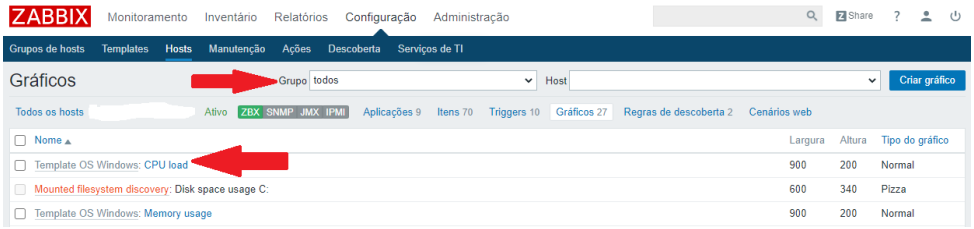

Fig. 13. Seleção de gráfico ”CPU Load”.

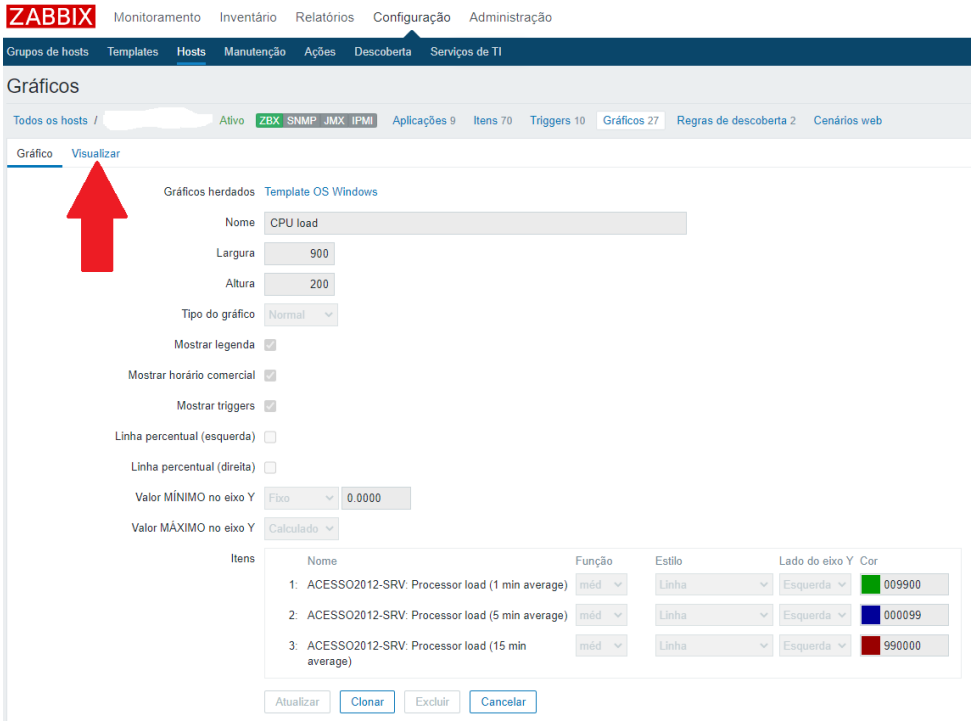

Fig. 14. Tela de configuração das características do gráfico.

Fig. 15. Visualização do gráfico ”CPU Load”.

Na tela seguinte, seleciona-se o item “Todos”para acesso aos vários modelos de gráficos que estão associados ao *template* selecionado, como visto na Figura 13.

Para o dispositivo MS Windows 10 Pro, seleciona-se um gráfico de “CPU Load” na Figura 13. Essa ação habilita uma tela para edição de diversas propriedades do gráfico.Ajustam-se controles de nome de exibição, dimensão do gráfico (largura x altura), cores fundamentais, inclusão de legendas, horários, porcentagens, etc. Na Figura 14, visualizam-se essas opções.

Para visualizar o gráfico, seleciona-se “Visualizar”como indicado na Figura 14. Na Figura 15, tem-se o gráfico de dados de consumo de processamento do dispositivo MS Windows 10 dentro de uma janela de tempo definida como padrão pelo Zabbix. Geralmente, as configurações padrão do servidor trazem parâmetros de desempenho dos últimos 1, 5, 15 e 60 minutos de uso do processador.

V. Conclusão

Este trabalho apresenta um breve tutorial sobre o uso do sistema de monitoramento Zabbix, sendo um resumo de um caderno de experimentos práticos desenvolvido pelos autores para o Laboratório de gerência de redes e segurança cibernética do Instituto Nacional de Telecomunicações. Além das funcionalidades abordadas nesse trabalho, ressalta-se que o sistema de monitoramento Zabbix possui um universo imenso de possibilidades de utilização no contexto de monitoramento, gerenciamento, alerta de incidentes de indisponibilidade, alertas preditivos de indisponibilidade e auxílio no monitoramento de alguns incidentes de segurança.

O sistema de monitoramento Zabbix também permite integrar a tomada de decisões básicas com a aplicação de controles de inteligência artificial e aprendizado de máquinas em relação ao comportamento de conexão de rede, consumo de memória, processamento e armazenamento. Portanto, propõem-se como trabalhos futuros pesquisas para integração de controles inteligentes ao sistema Zabbix por meio da linguagem Python.

Referências

[1] Rihards Olups Patrik Uytterhoeven. *Zabbix 4 Network Monitoring - Third Editions*. 3th. Packt, 2019.

[2] Bin Xiao e Weifeng Wang. "Intelligent network operation and maintenance system based on big data". Em: *Journal of Physics: Conference Series* 1744.23 (2021), pp. 873–879.

[3] E. da S. Rocha *et al*. "Aggregating data center measurements for availability analysis". Em: *Journal of Software: Practice and Experience* (2020), pp. 1–25. DOI: 10.1002/spe.2934.

[4] Jim Kurose e Keith Ross. *Redes de Computadores e a Internet: Uma Abordagem Top-Down*. 6th. Pearson, 2013.

[5] Zabbix Community. *Zabbix Documentation 3.0*. URL: https://www.zabbix.com/documentation/3.0/manual (acesso em 23/05/2020).