REVISTA FOCO
Interdisciplinary Studies
e-issn: 1981-223X

A IMPLEMENTAÇÃO DO ZABBIX COM SEGURANÇA: UM ESTUDO DE CASO ZABBIX SAFELY

IMPLEMENTING ZABBIX SECURELY: A ZABBIX SAFELY CASE STUDY

LA IMPLEMENTACIÓN DE ZABBIX DE FORMA SEGURA: UN ESTUDIO DE CASO ZABBIX CON SEGURIDAD

Roger Assunção da Silva[1]
Wagner José da Silva[2]

DOI: 10.54751/revistafoco.v17n4-055
Received: March 13th , 2024
Accepted: April 01st, 2024

RESUMO
O Zabbix é uma ferramenta de monitoramento de redes de dados, com ela é possível monitorar diversos dispositivos dentro da rede. Monitorar a rede de dados é essencial para qualquer empresa, independentemente de seu porte ou ramo de atuação, para garantir a segurança das informações e a continuidade de suas operações. Com o Zabbix podemos monitorar praticamente qualquer ativo que esteja conectado à rede de dados, sejam equipamentos ou serviços, e a partir desse monitoramento saber se o ativo está ligado, operacional e se apresenta algum comportamento que sugira problemas em seu funcionamento. De posse das informações é possível configurar a ferramenta de monitoramento para que execute alguma ação pré-definida, como emitir alertas ao gerente de redes ou executar algum comando remotamente e assim ter ações preventivas e corretivas mais assertivas. Os sistemas de monitoramento permitem também que os dados coletados sejam configurados e exibidos em dashboards para acompanhamento em tempo real, seja por meio do próprio Zabbix ou de aplicações específicas para a criação de visualizações gráficas como o Grafana.

Palavras-chave: Zabbix; monitoramento de rede de dados; gerenciamento de redes de dados.

ABSTRACT
Zabbix is a network monitoring tool which you can monitor several devices within the network. Monitoring data on a network is essential for any company, regardless of its size or industry, to ensure information security and the continuity of its operations. With Zabbix we can monitor practically any asset that is connected to the data network, whether equipment or services, and from this monitoring we can know whether the asset is connected, operational and

[1] Graduando em Tecnologia de Segurança da Informação pela Faculdade de Tecnologia da Informação Ministro Ralph Biassi (FATEC Americana). Rua Emílio de Menezes, S/N, Vila Amorim, Americana - SP, CEP: 13469-111.
E-mail: roger.silva23@fatec.sp.gov.br
[2] Mestre em Tecnologia. Faculdade de Tecnologia da Informação Ministro Ralph Biassi (FATEC Americana). Rua Emílio de Menezes, S/N, Vila Amorim, Americana - SP, CEP: 13469-111. E-mail: wagner.silva@fatec.sp.gov.br

whether it exhibits any behavior that suggests problems in its functioning. Once you have the information, it is possible to configure the monitoring tool to perform a pre-defined action, such as issuing an alert to the network manager or executing a command remotely and thus taking more preventive and corrective assertive actions. Monitoring systems also allow collected data to be configured and displayed on dashboards for real-time monitoring, through Zabbix itself or specific applications for creating graphical visualizations such as Grafana.

Keywords: Zabbix; data network monitoring; data network management.

RESUMEN
Zabbix es una herramienta de monitoreo de redes de datos que permite monitorear diversos dispositivos dentro de la red. Monitorear la red de datos es esencial para cualquier empresa, independientemente de su tamaño o sector, para garantizar la seguridad de la información y la continuidad de sus operaciones. Con Zabbix, podemos monitorear prácticamente cualquier activo conectado a la red de datos, ya sean equipos o servicios, y a partir de este monitoreo saber si el activo está encendido, operativo y si presenta algún comportamiento que sugiera problemas en su funcionamiento. Con la información recopilada, es posible configurar la herramienta de monitoreo para ejecutar alguna acción predefinida, como enviar alertas al gerente de redes o ejecutar algún comando de forma remota, y así llevar a cabo acciones preventivas y correctivas más efectivas. Los sistemas de monitoreo también permiten configurar y mostrar los datos recopilados en paneles de control para su seguimiento en tiempo real, ya sea a través de Zabbix mismo o de aplicaciones específicas para crear visualizaciones gráficas como Grafana.

Palabras clave: Zabbix; monitoreo de redes de datos; gestión de redes de datos.

1. Introdução

Este estudo de caso foi realizado em uma empresa de tecnologia da informação que fornece soluções de gestão comercial para empresas do ramo da construção civil localizadas em diversos municípios da região metropolitana de Campinas – RMC e da região metropolitana de Piracicaba – RMP, no interior do Estado de São Paulo – SP.

Cada empresa cliente possui sua própria infraestrutura de dados, composta geralmente por servidores de dados e infraestrutura de rede, todas com configurações de hardware e software distintos e executando outras aplicações além da aplicação fornecida pela empresa de sistema de gestão comercial. Na medida em que a quantidade de clientes aumenta fica mais difícil fazer a gestão do sistema instalado nos clientes, visto a distância geográfica entre um cliente e outro e as disparidades existentes entre as diversas configurações dos equipamentos.

O tempo de atendimento e de solução de problemas nos clientes é um fator crítico, já que uma falha pode prejudicar e até paralisar as operações de vendas, causando grandes prejuízos.

Com foco nessas características propôs-se a implantação de um sistema de monitoramento remoto dos equipamentos e serviços em execução nos clientes, com dois objetivos iniciais: prever possíveis problemas e agir preventivamente para que não aconteçam; identificar rapidamente as falhas e ter informações que permitam uma atuação rápida e assertiva por parte da equipe técnica. Ambos os objetivos visam reduzir ao máximo as ocorrências de indisponibilidade dos serviços tendo uma ação ativa da equipe técnica, que até então atua mediante solicitação dos clientes.

2. Desenvolvimento

O primeiro passo para buscar uma ferramenta que atendesse às necessidades da empresa foi elencar quais serviços deveriam ser monitorados, e a partir de discussões entre a equipe técnica foram elencados os seguintes itens como essenciais a serem monitorados para atingir os objetivos: hardware do cliente, englobando memória RAM, utilização do disco rígido, processamento, temperatura de trabalho; conectividade e funcionamento do gerenciador de banco de dados firebird; conectividade com a rede de dados (icmp); execução de aplicativos e processos pertinentes ao sistema de gestão comercial; quantidade de usuário utilizando o servidor de dados simultaneamente; conexão com a internet. Por se tratar de informações comerciais e financeiras as trocas de informações devem ser feitas de forma segura, por isso é utilizada a tecnologia Virtual Private Network – VPN ou rede virtual privada por meio da aplicação hamachi. É necessário que este serviço de proteção também seja monitorado pela aplicação a ser escolhida.

Após pesquisa por ferramentas de monitoramento de redes de dados disponíveis que atendessem aos requisitos elencados, optou-se pela ferramenta Zabbix, por ser gratuita, de código aberto e uma das ferramentas mais utilizadas para esse fim atualmente, além de ter documentação completa e em português disponível no site da ferramenta. De acordo com De Oliveira (2023) várias empresas estão utilizando softwares de código aberto em decorrência de sua qualidade e por

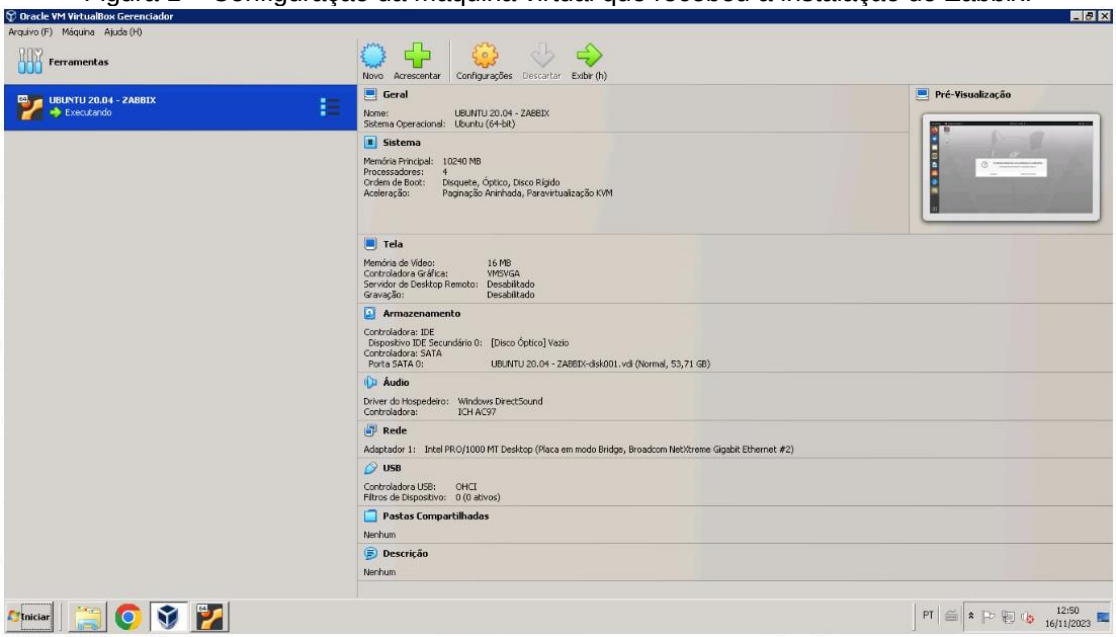
questões orçamentárias. No caso da empresa em que o estudo foi realizado, ambas as justificativas se aplicam. Aguiar (2017) relata em seu estudo, inclusive, que o Zabbix é utilizado pela Força Aérea Brasileira, tamanha sua robustez e qualidade.

O Zabbix é uma plataforma de monitoramento amplamente utilizada para supervisionar o desempenho, a disponibilidade e a integridade de redes, servidores e outros dispositivos de infraestrutura. Fornece uma solução abrangente para monitorar ambientes de TI e é projetado para ajudar as organizações a manterem o controle de seus ativos e garantir a eficiência operacional. A plataforma coleta dados em tempo real sobre o desempenho dos sistemas, permitindo a análise instantânea e a tomada de decisões rápidas, além de oferecer recursos de automação para simplificar tarefas rotineiras e suportar escalabilidade para ambientes que exigem monitoramento em grande escala.

De Barros (2022) esclarece que o Zabbix é uma ferramenta de monitoramento de rede criada pela Zabbix SIA, uma empresa criada por Alexei Vladishev em 1998. É capaz de rastrear e monitorar a rede de servidores, computadores, switches, roteadores, máquinas virtuais, serviços, aplicativos, sites, bancos de dados e até serviços em nuvem. Um de seus diferenciais é o eficiente e versátil sistema de notificações, o que proporciona uma resposta rápida a problemas.

Por não dispor de equipamento exclusivo para as ferramentas de monitoramento, o Zabbix foi instalado em uma máquina virtual utilizando o virtualizador gratuito VM VirtualBox, da empresa Oracle. Como pode ser observado na figura 1, a máquina virtual foi configurada com 10240 MB de memória RAM, com 4 processadores e 53 GB de armazenamento dinamicamente alocado. O sistema operacional escolhido foi o Ubuntu versão 20.04 de 64 bits.

Figura 1 – Configuração da máquina virtual que recebeu a instalação do Zabbix.



Fonte: Autoria própria.

A versão do Zabbix instalada foi a 6.09 LTS com banco de dados MySQL e web server Nginx. A sigla LTS significa Long Time Support, que no caso do Zabbix fornece suporte para a versão por até 5 anos após o lançamento. Optou-se por não instalar a versão mais atual por considerar a penúltima versão mais estável e segura.

Segundo Tebaldi (2014) o bom gerenciamento de redes envolve também o uso de softwares que coletam dados e criam mecanismos de comunicação entre o gerente de monitoramento e o agente coletor de dados.

Apesar de também conseguir coletar dados sem a necessidade desses agentes instalados nos clientes, já que tem suporte ao protocolo de coleta de dados SNMP, o Zabbix fornece a aplicação Zabbix Client, que instalado no equipamento a ser monitorado amplia muito a quantidade de informações que podem ser coletadas e monitoradas daquele ativo. Por esse motivo optou-se por instalar o Zabbix Client nos clientes a serem monitorados remotamente.

A etapa seguinte consistiu em adicionar itens para monitoramento e realizar testes para verificar a configuração ideal a ser utilizada. Os testes foram realizados com o monitoramento de equipamentos e serviços dentro da própria empresa de tecnologia, com esse monitoramento já foi possível identificar pontos de melhoria nos equipamentos dos funcionários que poderiam melhorar a dinâmica dos trabalhos prestados.

Ao seguir para a etapa de instalação nos clientes remotos houve falhas ao buscar informações de monitoramento já que os equipamentos a serem monitorados não estavam na mesma rede de dados. Após pesquisas e consultas a ferramentas de inteligência artificial percebeu-se a necessidade de utilizar conexão segura para monitorar os dados remotos, por isso foi necessária a configuração de uma rede virtual privada – Virtual Private Network (VPN).

Iniciou-se uma pesquisa por uma ferramenta de VPN que funcionasse bem com sistema operacional Linux ou Windows, já que estes eram os possíveis cenários nos clientes a serem monitorados. A ferramenta escolhida foi o Hamachi, que além de atender as necessidades do projeto possui interface gráfica para o sistema operacional utilizado, o Ubuntu 20.04. Essa foi uma das etapas mais demoradas e trabalhosas do projeto.

Logo em seguida iniciou-se a configuração do monitoramento dos dados coletados dos clientes, juntamente com a configuração de ações (triggers) e alertas. No entanto a visualização das informações com o Zabbix não atendia as necessidades previstas nos objetivos iniciais. Decidiu-se por buscar uma ferramenta de visualização de informações em dashboards para integrar ao Zabbix. Após pesquisas a ferramenta escolhida para criar as visualizações foi o Grafana, por ser uma ferramenta gratuita, completa em termos de visualização e bastante fácil de instalar e utilizar.

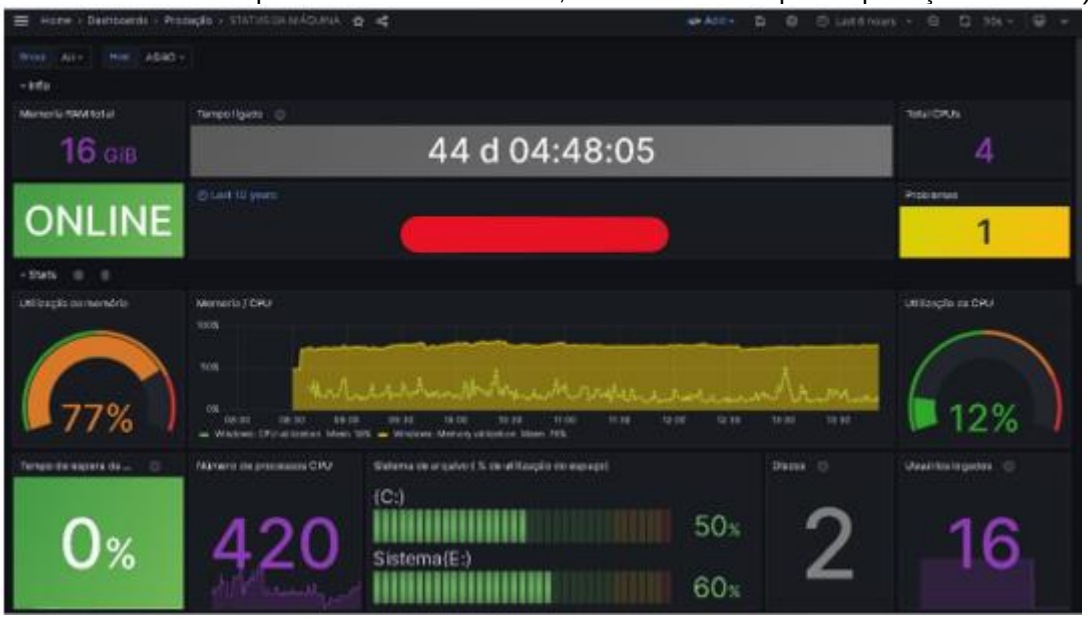
A integração do Zabbix com Grafana permitiu a criação de dashboards intuitivos e funcionais, que permitem a visualização rápida dos dados dos equipamentos instalados nos mais de 50 clientes atendidos pela empresa de tecnologia. A seguir alguns exemplos dos dashboards configurados:

Na Figura 2 é possível verificar o dashboard que mostra de forma simples de muito rápida o status dos servidores de dados instalados nos clientes. Caso um dos clientes tenham seu equipamento desligado, imediatamente aparecerá o texto “Desligado” na cor vermelha, permitindo à equipe técnica uma ação ativa e rápida para retomar o funcionamento do equipamento e dos serviços.

Figura 2 – Monitoramento do status do servidor de dados(A parte em vermelho é o local em que fica o nome do cliente, não foi mostrado para a proteção de dados).

Fonte: Autoria própria.

Figura 3 – Dashboard por cliente para ver o status geral do servidor monitorado. (A parte em vermelho é o local em que fica o nome do cliente, não foi mostrado para a proteção de dados).



Fonte: Autoria própria.

No dashboard apresentado na Figura 3 é possível monitorar o estado geral de cada um dos servidores, tendo de forma simples e em uma mesma interface informações sobre uso e memória RAM, uso da capacidade de processamento, conectividade com a internet, CPU´s em funcionamento, tempo de funcionamento ininterrupto do equipamento, quantidade processos em execução, quantidade de

discos rígidos disponíveis, uso do espaço para armazenamento de dados e usuário logados simultaneamente. Estes dados permitem aos técnicos detectar situações de alerta e atuar preventivamente, reduzindo a possibilidade de parada dos serviços. Na tela apresentada, por exemplo o uso de memória RAM está próximo ao limite para atuação ativa dos técnicos, já que a ferramenta foi configurada para gerar um alerta de risco com 80% de uso da memória RAM e o sistema apresenta 77% de uso.

A interface apresenta ainda a quantidade de erros reportados para aquele servidor, no entanto essa informação não necessariamente representa um problema, já que a ferramenta procura por informações que não estão disponíveis em todos os equipamentos, dada a heterogeneidade de suas configurações. É possível que o técnico verifique os problemas reportados para checar se algum se refere aos serviços essenciais para funcionamento da ferramenta de gestão que a empresa de tecnologia fornece.

A Figura 4 mostra a interface onde os erros são reportados e o técnico pode verificar com precisão qual o erro reportado.

Figura 4 – Interface de erros reportados (A parte em vermelho é o local em que fica o nome do cliente, não foi mostrado para a proteção de dados).

Fonte: Autoria própria.

Com a união das ferramentas Zabbix e Grafana é possível criar uma diversidade enorme de visualizações de monitoramento, levando em conta as possibilidades das ferramentas e características do projeto em desenvolvimento.

3. Resultados

Os objetivos pretendidos foram alcançados com o uso das ferramentas de monitoramento remoto, uma vez que com a visualização dos dashboards é possível verificar situações propensas a causar um problema de funcionamento nos equipamentos dos clientes e agir preventivamente para solucionar estas situações, quando não for possível evitar o problema, a equipe pode atuar de forma muito mais rápida e assertiva na solução do problema, visto que possuem informações precisas e em tempo real do funcionamento do equipamento e dos softwares que estão em execução.

Além de influenciar positivamente na imagem da empresa de tecnologia, a empresa ganha em produtividade e economia, pois vários problemas que necessitavam do deslocamento de um técnico até o cliente podem ser resolvidos remotamente.

É possível ainda, a partir dos dados observados, emitir relatórios aos clientes sobre suas infraestruturas de TI, e com isso permitir e orientá-los sobre o melhor uso dos recursos ou sobre a necessidade de investimentos para melhorar sua experiência no uso das ferramentas contratadas.

Percebeu-se a necessidade de melhorar a configuração do monitoramento de forma personalizada para cada cliente para que o Zabbix ignore falsos alertas de erros, que na verdade são itens monitorados que não estão disponíveis nos equipamentos daquele cliente.

4. Conclusão

Possuir um sistema de monitoramento remoto de redes é muito útil em situações em que os clientes estão geograficamente espalhados. Os principais ganhos estão relacionados à satisfação do cliente em ser atendido rapidamente ou mesmo ter os problemas resolvidos sem cause nenhum impacto às suas operações.

Trabalhar com monitoramento remoto facilita e agiliza bastante o trabalho da equipe técnica, já que consegue monitorar em tempo real o que está acontecendo em cada equipamento do qual é responsável.

O processo de escolha, instalação e configuração das ferramentas utilizadas neste projeto foram essenciais para o aprendizado da equipe, e permitiram que muitas outras possibilidades fossem exploradas.

Como etapa seguinte pretende-se criar visualizações de acesso independente para que cada cliente possa monitorar seus próprios equipamentos.

REFERÊNCIAS

AGUIAR, I.F. (2017). **Proposta de utilização da ferramenta Zabbix no gerenciamento de redes: um estudo de caso no ambiente da FAB segundo boas práticas de governança de TI.** Orientadora: Moacyr Henrique Cruz de Azevedo. TCC (Graduação) – Curso de Ciência da Computação, Universidade Federal do Rio de Janeiro. Disponível em: https://pantheon.ufrj.br/handle/11422/3300. Acesso em: out/2023.

DE BARROS, Francisco Fernandes Xavier. **Advanced Oracle monitoring agent for Zabbix.** 2022. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/145449/2/592026.pdf. Acesso em: nov/2023.

DE OLIVEIRA, Felipe Barreto et al. **Aplicação de Melhores Práticas de Gestão e Segurança para Monitoração de Ativos de Infraestrutura.** Revista Ibérica de Sistemas e Tecnologias de Informação, n. E62, p. 333-346, 2023. Disponível em: https://media.proquest.com/media/hms/PFT/1/FFtxV?_s=RHAIE9IlCD8g5VDlNiujVICfAM0%3D. Acesso em: nov/2023.

TEBALDI, P. C. **Monitoramento de rede: como fazer?** Blog OPServices. 2014. Disponível em: https://www.opservices.com.br/monitoramento-de-rede. Acesso em: out/2023.

UNIREDE (2023). **Monitoramento de redes, o que é?** Portal de Conhecimento da Empresa Unirede – inteligência em TI. Disponível em: https://www.unirede.net/monitoramento-de-rede-o-que-e/. Acesso em: nov/2023.