***CAMPUS* PORTO VELHO ZONA NORTE**
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

ADELZEMIR DOS SANTOS SOUZA SILVA
MARIA JOSÉ OLIVEIRA DOS SANTOS

ESTUDO DE GERENCIAMENTO DE REDES COM ZABBIX SERVER

PORTO VELHO
2024

ADELZEMIR DOS SANTOS SOUZA SILVA
MARIA JOSÉ OLIVEIRA DOS SANTOS

ESTUDO DE GERENCIAMENTO DE REDES COM ZABBIX SERVER

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores pelo Instituto Federal de Educação, Ciência e Tecnologia de Rondônia– Campus Porto Velho Zona Norte.

Orientador: Prof. Me. Renato Almeida de Oliveira

PORTO VELHO
2024

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO, com dados informados pelo(a) próprio(a) autor(a).

Silva, Adelzemir dos Santos Souza.
Estudo de gerenciamento de redes com Zabbix Server / Adelzemir dos Santos Souza Silva, Maria José Oliveira dos Santos, Porto Velho-RO, 2024.
24 f.

Orientador(a): Prof. Me. Renato Almeida de Oliveira.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho-RO, 2024.

1. Gerenciamento de redes. 2. Protocolos. 3. Zabbix Server. I. Santos, Maria José Oliveira dos. II. Oliveira, Renato Almeida de (orient.). III. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. IV. Título.

Bibliotecário(a) Responsável: Celia Reis Sales, CRB-CRB11/955 (Campus Porto Velho Zona Norte)

Estudo de gerenciamento de redes com Zabbix Server

Network management study with Zabbix Server

Estudio de gestión de red con Zabbix Server

DOI:10.38152/bjtv7n4-001

Submitted: Aug 23th,, 2024
Approved: Sep 13th, 2024

Adelzemir dos Santos Souza Silva
Graduado em Tecnologia em Redes de Computadores
Instituição: Instituto Federal de Rondônia - campus Zona Norte
Endereço: Porto Velho, Rondônia Brasil
E-mail adelzemir@gmail.com

Maria José Oliveira dos Santos
Graduada em Tecnologia em Redes de Computadore
Instituição: Instituto Federal de Rondônia - campus Zona Norte
Endereço: Porto Velho, Rondônia, Brasil
E-mail: maryaoliveira59@gmail.com

Renato Almeida de Oliveira
Mestre em Administração pela Fundação Universidade Federal de Rondônia (UNIR)
Instituição: Instituto Federal de Rondônia - campus Porto Velho Zona Norte
Endereço: Porto Velho, Rondônia, Brasil
E-mail: renato.oliveira@ifro.edu.br

RESUMO
Este artigo aborda o uso do sistema Zabbix Server e suas configurações e os elementos utilizados para o monitoramento, analisando através de livros, vídeos e documentos técnicos. Os resultados mostram que o Zabbix oferece funcionalidades abrangentes, como monitoramento em tempo real, alertas configuráveis e dashboards personalizados, além de flexibilidade e escalabilidade. Entretanto, a implementação eficaz requer planejamento cuidadoso e ajustes contínuos. Este estudo fornece orientações práticas para otimizar o uso do Zabbix, contribuindo para uma infraestrutura de TI mais estável e eficiente.

Palavras chave: gerenciamento de redes, protocolos, Zabbix Server.

ABSTRACT
This article discusses the use of the Zabbix Server system and its configurations and the elements used for monitoring, analyzing books, videos and technical documents. The results show that Zabbix offers comprehensive functionality, such as real-time monitoring, configurable alerts and personalized dashboards, as well as flexibility and scalability. However, effective implementation requires careful planning and continuous adjustments. This study provides practical guidance for optimizing the use of Zabbix, contributing to a more stable and efficient IT infrastructure.

Keywords: network management, protocols, Zabbix Server.

RESUMEN
Este artículo analiza el uso del sistema Zabbix Server y sus configuraciones y los elementos utilizados para monitorear, analizar libros, videos y documentos técnicos. Los resultados muestran que Zabbix ofrece una funcionalidad integral, como monitoreo en tiempo real, alertas configurables y paneles personalizados, así como flexibilidad y escalabilidad. Sin embargo, una implementación efectiva requiere una planificación cuidadosa y ajustes continuos. Este estudio proporciona una guía práctica para optimizar el uso de Zabbix, contribuyendo a una infraestructura de TI más estable y eficiente.

Palabras clave: gestión de red, protocolos, Zabbix Server.

1 INTRODUÇÃO

No atual cenário da Tecnologia da Informação e Comunicação (TIC), uma gestão eficaz de infraestrutura é de suma importância para garantir a continuidade e a qualidade dos serviços oferecidos pelas organizações. O monitoramento de rede e sistemas desempenha um importante papel, possibilitando a detecção de falhas e a resolução de problemas, garantindo a disponibilidade dos sistemas monitorados. O Zabbix Server se destaca como uma das ferramentas mais poderosas e flexíveis para o monitoramento de infraestrutura de redes de computadores.

O tema da pesquisa se delimitou às configurações do Zabbix Server onde foram abordadas as etapas de instalação e configuração, incluindo a definição de hosts, itens, triggers, templates e a configuração de alertas, além de explicar os protocolos por ele utilizado para realizar as coletas dos dados do hosts alvo do monitoramento.

A justificativa da pesquisa se deu pela constatação da crescente complexidade das infraestruturas de TI e da necessidade crítica de ferramentas eficazes para o monitoramento e gerenciamento de sistemas. Neste cenário o Zabbix Server se destaca como uma solução de monitoramento robusta e de código aberto que oferece uma gama de funcionalidades para a detecção proativa de problemas, coleta e análise de dados de desempenho, e alertas em tempo real.

Baseado em um pressuposto teórico que ressalta a importância do Zabbix Server como uma ferramenta muito relevante para um monitoramento eficaz e a gestão de infraestruturas de TI, e traz um conjunto de ideias, teorias, conceitos de autores como James KUROSE, FOROUZAN, Janssen L Reis, Andrew S. Tanenbaum e M Soares além da própria documentação do Zabbix que explica os mais variados detalhes de cada componente e suas configurações.

Este estudo concentra-se na análise do uso e aplicação do Zabbix Server no

monitoramento de infraestrutura de TI, abordando suas configurações, e elementos que utiliza para realizar o monitoramento de outros sistemas. A pesquisa se limita a um estudo prático/teórico do Zabbix Server no monitoramento de redes de computadores e foi aplicado no Laboratório de Redes do IFRO Zona Norte em Máquinas Virtuais isoladas da rede principal para não afetar o funcionamento da instituição.

Também é objetivo explicar o que é o Zabbix Server e como ele funciona, proporcionando uma compreensão das suas características, funcionamento e uso no campo, explorando as suas capacidades que podem ser plenamente aproveitadas.

O estudo será conduzido por meio de uma abordagem de pesquisa descritiva, com o objetivo de compreender e interpretar os detalhes, experiências e percepções em relação ao monitoramento de redes utilizando o Zabbix. Esta pesquisa descritiva permitirá uma análise detalhada das práticas, desafios e benefícios observados durante o uso do Zabbix Server, fornecendo uma visão abrangente sobre sua eficácia e aplicação prática no contexto do monitoramento de redes de computadores.

2 REFERENCIAL TEÓRICO

2.1 GERENCIAMENTO DE REDE DE COMPUTADORES

Gerenciamento de rede de computadores refere-se à implementação de software para monitoramento e manutenção de uma infraestrutura de rede para garantir que os recursos de rede estejam operando de forma eficiente, confiável e conforme as necessidades da organização e de seus usuários. Este software deve ser capaz de realizar o monitoramento e supervisão de todos os componentes da rede, incluindo dispositivos de rede, servidores, sistemas de armazenamento, aplicativos e serviços.

> Gerenciamento de rede inclui a implementação, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço a um custo razoável (Kurose, Ross, 2013, p. 558).

Gerenciamento de desempenho de redes de computadores é uma prática essencial para garantir o funcionamento adequado e consistente de uma infraestrutura de rede. Envolve a monitorização, análise e otimização dos recursos de rede para garantir um desempenho adequado e satisfatório. Na análise de desempenho, os dados de monitorização são fundamentais para identificar gargalos, padrões de utilização, pontos fracos e áreas que

necessitam de melhorias. As informações coletadas podem ser usadas para identificar problemas de congestionamento, latência, perdas de pacotes, e outros fatores que podem afetar o desempenho da rede.

De acordo com Forouzan (2008), gerenciamento de desempenho está intimamente relacionado ao gerenciamento de falhas, tentar monitorar e controlar a rede para garantir que ela esteja rodando da forma mais eficiente possível.

Com a utilização de ferramentas de monitoramento como o Zabbix Server, para acompanhar o estado da rede, identificar falhas ou eventos anormais, o administrador pode voltar ao funcionamento normal da rede o mais rápido possível, garantindo a disponibilidade e a confiabilidade dos serviços para os usuários finais.

A arquitetura de um sistema de gerenciamento de rede (Network Management System - NMS) em sua maioria segue uma arquitetura básica composta pelos seguintes componentes, entidade gerenciadora, dispositivo gerenciado e protocolos de gerenciamento de redes.

Entidade gerenciadora é responsável pelo gerenciamento e controle dos dispositivos e recursos da rede, podendo ser uma ferramenta de software ou um sistema que realiza várias tarefas relacionadas ao gerenciamento da rede.

Estas entidades desempenham um papel muito importante no monitoramento, configuração, solução de problemas e otimização de redes de computadores, fornecendo uma visão centralizada dos dispositivos e recursos da rede, permitindo uma administração eficiente e garantindo a disponibilidade e o desempenho adequados de uma rede de computadores.

A entidade gerenciadora é uma central responsável por controlar a coleta, processamento, análise e apresentação de informações de gerenciamento de rede (KUROSE, ROSS, 2013, p. 559).

Dispositivos gerenciáveis em redes de computadores referem-se aos dispositivos que possuam um ip na rede e que possa ser monitorado, configurado e controlado por uma entidade de gerenciamento ou uma ferramenta de monitoramento, quaisquer dispositivos que possuam tais características são considerados dispositivos gerenciados.

De acordo com Kurose (2013), dispositivos gerenciáveis em uma rede de computadores possuem um agente de gerenciamento de rede, que tem a função de estabelecer conexão com a entidade gerenciadora e realizar ações específicas nos dispositivos sob sua supervisão, de acordo com as instruções que recebe.

Protocolos de Gerenciamento são usados para trocar informações entre a estação de gerenciamento e os agentes nos dispositivos de rede.

2.2 PROTOCOLO SNMP

O SNMP (Simple Network Management Protocol) é um protocolo de rede muito utilizado para o gerenciamento e monitoramento de dispositivos de rede. Ele é projetado para facilitar a troca de informações entre os elementos gerenciadores (gerentes) e os dispositivos gerenciados (agentes) em uma rede. O protocolo SNMP opera usando o modelo cliente/servidor, onde o gerente envia solicitações aos agentes para obter informações de gerenciamento e os agentes respondem a essas solicitações.

Este protocolo é muito utilizado no gerenciamento de redes, permitindo que os administradores monitorem o desempenho da rede, configurem dispositivos remotamente, coletem informações de gerenciamento e detectem falhas. É usado em uma variedade de dispositivos de rede, como roteadores, switches, firewalls, servidores e dispositivos de armazenamento.

De acordo com Forouzan (2008) o SNMP é um protocolo de aplicação que permite a estações-gerentes monitorarem agentes em dispositivos de diferentes fabricantes e redes.

Gerentes SNMP são os sistemas ou aplicações responsáveis por monitorar e gerenciar dispositivos de rede que enviam solicitações SNMP aos agentes para obter informações sobre o status, configuração e desempenho dos dispositivos. Os gerentes processam as respostas dos agentes e podem tomar ações com base nas informações coletadas.

Agentes SNMP são componentes de software ou firmware instalados nos dispositivos de rede que fornecem informações gerenciadas. Estes agentes coletam e armazenam informações sobre o dispositivo, como status, métricas de desempenho, eventos e configurações, e depois respondem às solicitações dos gerentes e também podem enviar notificações de eventos para informar sobre condições específicas, como falhas ou alterações de estado.

> Uma estação gerenciadora, denominada gerente, é um host que roda o programa-cliente SNMP. Uma estação gerenciada, denominada agente, é um roteador (ou um host) que executa o programa-servidor SNMP. O gerenciamento é obtido pela interação entre gerente e agente (Forouzan 2008 p.878).

MIB (Management Information Base), é a estrutura de dados hierárquica que define as informações gerenciadas disponíveis em um dispositivo de rede, sua principal função é fornecer uma visão lógica e estruturada dos dispositivos gerenciados. Ela fornece quais informações podem ser acessadas e manipuladas pelos gerentes SNMP. A MIB especifica os tipos de dados, as propriedades e as relações entre os objetos gerenciados. As informações

são organizadas em uma árvore de objetos, onde cada objeto é identificado por um OID (Object Identifier).

OID (Object Identifier) é representado em uma sequência numérica única que identifica de forma exclusiva um objeto na MIB (Management Information Base) do SNMP, permite que os objetos gerenciados na MIB (Management Information Base) sejam identificados de maneira única, são representado no formato de sequência de números separados por pontos.

De acordo com Kurose (2013), um objeto MIB é uma entidade que pode representar informações variadas, como contagem de datagramas IP descartados devido a erros em cabeçalhos ou erros de detecção de portadora em uma interface Ethernet.

2.3 PROTOCOLO ICMP

ICMP (Internet Control Message Protocol) é um protocolo de comunicação que atua na camada de rede do modelo TCP/IP, tem como função fornecer informações de controle e de gerenciamento relacionadas à comunicação de rede.

ICMP Ping, também conhecido como "ping", é uma ferramenta de protocolo de rede que utiliza pacotes ICMP (Internet Control Message Protocol) para verificar a conectividade entre os mais variados dispositivos em uma rede. O ping é amplamente utilizado para testar a conectividade, medir o tempo de resposta e verificar a disponibilidade de um host.

Quando um comando de ping é enviado de um dispositivo para outro, um pacote ICMP Echo Request é enviado para o destino. O dispositivo de destino recebe o pacote ICMP e, se estiver ligado e habilitado para responder a pings, envia um pacote ICMP Echo Reply de volta ao dispositivo de origem.

> As mensagens ECHO e ECHO REPLY são usadas para verificar se um determinado destino está ativo e acessível. Ao receber a mensagem ECHO, o destino deve enviar de volta uma mensagem ECHO REPLY. As mensagens TIMESTAMP REQUEST e TIMESTAMP REPLY são semelhantes, exceto pelo fato de o tempo de chegada da mensagem e o tempo de saída da resposta serem registrados na mensagem de resposta. Esse recurso é usado para medir o desempenho da rede (Andrew S. Tanenbaum 2003, p. 346).

O tempo decorrido entre o envio do pacote ICMP Echo Request e a recepção do pacote ICMP Echo Reply é conhecido como tempo de ida e volta (round-trip time, RTT). O protocolo ICMP pode relatar erros ou condições anormais encontradas durante a transmissão de pacotes. Por exemplo, quando um pacote não puder ser entregue ao destinatário, um pacote ICMP de destino inalcançável é enviado de volta ao dispositivo de origem,

informando sobre a falha na entrega.

> A mensagem DESTINATION UNREACHABLE é utilizada quando a sub-rede ou um roteador não consegue encontrar o destino, ou quando um pacote com o bit DF não pode ser entregue devido à presença de uma rede de "pacotes pequenos" no caminho (Andrew S. Tanenbaum 2003, p. 346).

O Zabbix Server, como Servidor de Monitoramento, pode ser configurado para medir e registrar o tempo de resposta ICMP usando itens específicos de ICMP. Isso permite monitorar o tempo de resposta entre hosts e diagnosticar problemas de conectividade e latência na rede.

2.4 ARQUITETURA E COMPONENTES DO ZABBIX

A instalação do Zabbix pode ser All in One (Tudo em Um), onde envolve a instalação de todos os componentes necessários em uma única máquina onde o Zabbix Server, o Banco de Dados e Frontend são todos instalados em um só servidor. Neste caso deve haver um certo cuidado, como verificar se existem recursos adequados (CPU, RAM, espaço em disco) para executar o Zabbix Server com Front End e Banco de Dados. Conforme Lima (2020, p. 7), "é possível separar os servidores web, servidor de banco de dados e servidor de monitoramento para aumentar a flexibilidade e ganhar em desempenho".

A arquitetura de duas camadas do Zabbix envolve separar o Zabbix Server e o Banco de Dados em duas máquinas diferentes, nesta abordagem é útil para o melhoramento de desempenho, escalabilidade e a disponibilidade do sistema, no servidor de Banco de Dado seu IP será apontando para Servidor Zabbix Server com Front End.

A instalação do Zabbix Server em três camadas, que envolve separar os componentes do Zabbix Server, banco de dados e Front End em diferentes servidores, com isso se cria um ambiente de alta performance, escalável e de alta disponibilidade.

Backend representado pelo Zabbix Server responsável por gerenciar a coleta e recebimento de dados, calcular os dados e enviar notificações aos usuários através de interfaces web, sms ou por e-mail, por exemplo.

Banco de Dados – Para iniciar a instalação do Zabbix Server se faz necessário ter feito a instalação do Banco de Dados. Ele é utilizado para armazenar os dados de configuração e dados de coletas de itens configurados do Zabbix, segundo Reis L. Janssen. (2020, p. 9) 'A camada de banco é representada pela a base de dados, que fica responsável por armazenar as informações coletadas pelo backend e apresentá-las ao frontend'.

Frontend - representada pela camada de interface web, a qual dá acesso às

informações de monitoramento, gerenciamento das configurações e fornece também informações para aplicações que utilizam a API do Zabbix.

> Zabbix Server é uma solução de código aberto que monitora vários parâmetros de redes, a saúde e integridade de servidores, máquinas virtuais, aplicações, serviços, banco de dados, websites, a nuvem e muito mais. O Zabbix usa um mecanismo flexível de notificação que permite aos usuários configurar alertas baseados em e-mail para praticamente qualquer evento. Isso permite uma resposta rápida para problemas do servidor (Zabbix Sia, 2023).

Servidor Zabbix é o componente principal da solução onde é instalado o Zabbix Server, este faz a gerência de todos os componentes da rede de computadores através da coleta e recebimento de dados enviados pelos os agentes zabbix ou snmp instalado nos hosts ou pelo envio do proxy, além de poder executar verificações remotas dos dispositivos monitorados através de verificações simples. O servidor gerencia o repositório central de configuração, estatísticas e armazenamento de dados operacionais, é ele que alerta os administradores quando os incidentes ocorrerem.

De acordo com Zabbix CIA (2024) o Zabbix Server é o núcleo da solução, gerenciando o repositório central de configuração e dados operacionais. Ele também monitora estatísticas e alerta os administradores em caso de incidentes.

Para a utilização do serviços do Zabbix server se faz necessário a instalação de três componentes: Zabbix Server, Interface Web e um Banco de Dados. O Zabbix Server pode ser instalado em servidores separados ou juntos de modo que todas as mudanças feitas na Interface Web irão refletir no Banco de Dados.

Zabbix Proxy - sua função é receber os dados dos hosts monitorados, armazenar temporariamente (buffer) e depois enviar ao servidor zabbix e após o envio desses dados ao servidor, esses mesmos dados são excluídos do proxy logo após o envio ao zabbix server. Em todo caso os agentes instalados nos hosts veem o Zabbix Proxy como se fosse o Servidor Zabbix. Sua utilização é opcional, mas em ambiente com um grande número de máquinas a serem monitoradas ou instaladas em localidades geograficamente diferentes é recomendado que faça sua utilização, pois caso o Servidor Zabbix pare seu funcionamento, além de receber os dados dos hosts para um envio posterior, ele faz um balanceamento de carga diminuindo uso de processamento por parte do Servidor Zabbix Server.

> O Zabbix Proxy é um processo que pode receber dados de um ou mais dispositivos monitorados e enviar ao Zabbix Server, basicamente ele funciona em nome do Zabbix Server (na visão do agente monitorado o Proxy passa a ser o Zabbix Server). Todo os dados recebidos são armazenados temporariamente (buferizados), transferidos ao Zabbix Server que o Zabbix Proxy pertencer, sendo excluídos na sequência do armazenamento temporário do Proxy (Zabbix Sia,

2024).

Zabbix Java Gateway - utilizado para monitorar máquinas Java, ele oferece suporte para monitoramento de aplicativos JMX, aceitando conexões de entrada do Servidor Zabbix ou Proxy Zabbix e só pode ser usado como um "proxy passivo" e funciona em processo de background ou seja quando Zabbix Server precisa de dados de coleta de um item JMX, em um host no zabbix server, quando solicita esses dados para Zabbix Java Gateway que possui a API de gerência JMX.

Quando o Zabbix Server precisa coletar um dado de um contador JMX em um host, ele faz a solicitação ao Zabbix Java Gateway, que utiliza a API de gerenciamento JMX para obter o dado desejado da aplicação (Zabbix Sia, 2024).

2.5 ELEMENTOS DE MONITORAMENTO ZABBIX SERVER

Host Zabbix - podem ser quaisquer equipamentos físicos ou virtuais conectados a uma rede que tenha um endereço IP, o qual se deseja monitorar seus serviços, para isso precisamos cadastrar no Zabbix Server em sua interface Web.

Podemos resumir a definição de host como sendo qualquer elemento de sua rede que possua um IP e tenha capacidade de comunicação com o Zabbix, seja através de coletas ativas ou passivas (ZABBIX SIA, 2024).

Itens são os elementos que definem os tipos de dados que irão ser coletados e quando serão coletados, são agrupados em hosts mas podem ser também definidos em um Template. Para cadastrar um item, precisamos informar um nome, um tipo do item, uma chave que definirá o tipo de informação que será coletada, a interface do host que será cadastrada no item, o tempo de coleta pode ser modificado após seu cadastro.

Os itens são essenciais para a coleta de dados no Zabbix, pois definem as métricas e os tipos de dados a serem coletados de um host (Zabbix Sia, 2024).

Item Passivo - Quando o host é configurado para enviar os dados de monitoramento para o Zabbix Server ou Zabbix Proxy automaticamente, em intervalos regulares e o Zabbix Server por sua vez faz os cálculos dos itens ou trigger e apresenta na interface web para que o administrador tome providências para resolução de problemas apresentado.

Item Ativo - é um software que será instalado nos hosts que se deseja monitorar, e ficará responsável pela coleta de dados de monitoramento dos sistemas hospedeiros para posterior envio ao Zabbix Server. Nas configurações de item ativo o Zabbix Server envia solicitações para os agentes instalados nos hosts para poder obter informações dos dados de

monitoramento.

SNMP - utilizado para monitorar dispositivos como impresoras, switches, roteadores ou nobreaks, permite a coleta de dados para monitoramento dos dispositivos no qual deverá se localizar o número de OID, este é uma sequência numérica que atua como um identificador único para cada tipo de dado que pode ser consultado no dispositivo, que se deseja monitorar e verificar qual o nome de comunidade configurada no dispositivo, esta comunidade por sua vez funciona como uma senha entre o dispositivo monitorado e o Zabbix Server, permitindo que o servidor faça um espécie de autenticação no dispositivo e colete os dados enviando até o servidor e que será apresentado na interface Web Zabbix.

Uma entidade SNMP armazena informações sobre direitos de acesso e políticas em um banco de dados de configuração local (Local Configuration Datastore — LCD) (Kurose, Ross, 2013, p. 572).

SNMP TRAP - em um snmptrap o dispositivo envia as informações para zabbix server ou zabbix proxy, um ponto importante deste item é que, não precisa esperar a próxima checagem do zabbix para obter informações do item, quando um dispositivo muda de status ou parar seu funcionamento, snmp traps são enviados com os dados de status de funcionamento do item.

De acordo com Forouzan (2008), as mensagens trap são utilizadas para informar uma entidade gerenciadora sobre uma situação excepcional que provocou alterações nos valores dos objetos MIB.

Verificações simples são tarefas de monitoramento que envolvem a coleta de informações básicas sobre hosts, serviços ou recursos, sem a necessidade de configurações complexas como a instalação e configuração de um agente no host alvo do monitoramento como por exemplo a verificação de disponibilidade feito com ICMP Ping.

Verificações simples são normalmente usadas para observações remotas de serviço, sem agente, neste caso o Zabbix Server/Proxy é responsável pelo processamento das verificações simples (Zabbix Sia, 2024).

HTTP agent - permite fazer o monitoramento de disponibilidade e desempenho de aplicações de um serviço web. A verificação de item HTTP é executada pelo servidor Zabbix, no entanto, quando os hosts são monitorados por um proxy Zabbix as verificações de itens HTTP são executadas pelo proxy (Zabbix Sia, 2024).

SSH/Telnet - permite que sejam executados remotamente em outro dispositivo monitorado usando o protocolo SSH ou Telnet, servindo para coletar informações como estatísticas de recursos (CPU, RAM, espaço em disco) ou o status de serviços em hosts remotos. Verificações SSH são executadas como monitoramento sem agente, essas

verificações SSH oferecem dois métodos de autenticação, um com par de usuário/senha e outro baseado em arquivo de chave (Zabbix Sia, 2024).

Trigger - (gatilho) é uma expressão lógica que define se os dados enviados por um item são aceitáveis ou não, caso não esteja dentro dos padrões aceitos, um alerta é acionado na interface do Zabbix para que o administrador de rede possa tomar uma providência em relação ao alerta informado. Na configuração da Trigger, geralmente se escolhe um nível de severidade para alertar o administrador de redes dos eventuais eventos, podendo ser desde o nível mais básico até no nível mais alto, por exemplo nível mais alto (Desastre) caso um servidor desligue irá acender um alerta vermelho.

> Os gatilhos são expressões lógicas que "avaliam" os dados reunidos por itens e representam o atual estado do sistema. Expressões de gatilho permitem definir um limite de que estado de dado é "aceitável". Portanto, caso um dado de entrada ultrapasse o estado aceitável, um gatilho é "disparado" - ou altera o estado para PROBLEMA (Zabbix Sia, 2024).

Template - é uma forma de padronizar um ambiente para monitoramento, agrupando-se um conjunto de serviços comuns e associando a um host, de forma que quando precisar monitorar outros hosts com as mesmas características não será preciso preocupar-se em fazer tudo do zero, é só associar este host ao template cadastrado, que o template fornece todos os serviços de monitoramento cadastrado no template a esse host.

> Modelos (templates) - um conjunto de entidades (itens, gatilhos, gráficos, regras de descoberta de baixo-nível, cenários web) prontas para serem aplicadas a um ou vários hosts. A função dos modelos é acelerar a implementação de tarefas de monitoramento em um host; também tornar mais fácil a aplicação de mudanças em massa às tarefas de monitoramento. Modelos são associados diretamente a hosts individualmente (Zabbix Sia, 2024).

Eventos são acontecimentos gerados por diferentes fontes no Zabbix. Em uma trigger, quando acontece uma mudança de estado, é gerado um evento e esse evento pode ser do tipo ‘PROBLEMA’ ou evento ‘OK’, sendo que o evento ‘PROBLEMA’ ocorre quando a coleta estiver com os dados fora dos padrões aceitáveis pela a trigger e o evento ‘OK’ ocorre quando uma nova coleta trazer dados dentro dos padrões aceitáveis pela a trigger.

> Os gatilhos são expressões lógicas que "avaliam" os dados reunidos por itens e representam o atual estado do sistema. Expressões de gatilho permite definir um limite de estado do dado que é "aceitável". Portanto, caso um dado de entrada ultrapasse o estado aceitável, um gatilho é "disparado" - ou altera o estado para PROBLEMA (Zabbix Sia, 2024).

Macros - São variáveis que substituem valores de acordo com o contexto que lhe são passados, identificadas por uma sintaxe específica, são escritas entre chaves e começam com um cifrão, os nomes são escrito em letras maiúsculas e são permitidos números de 0 a 9 além de underline (_) e o ponto(.).

3 METODOLOGIA

Esta pesquisa tem por finalidade o estudo do Zabbix Server no monitoramento de redes de computadores em uma abordagem descritiva sobre os principais componentes de monitoramento do sistema Zabbix, configuração do sistema e aplicação, simulando um ambiente real e realizando o monitoramento de hosts como switch e servidores.

A pesquisa descritiva é uma abordagem de investigação cujo objetivo principal é descrever as características, comportamentos, eventos, ou situações de um determinado fenômeno ou população. Em vez de explorar relações de causa e efeito ou testar hipóteses, a pesquisa descritiva se concentra em fornecer uma representação precisa e detalhada do que está sendo estudado.

> As pesquisas descritivas são, juntamente com as exploratórias, as que habitualmente realizam os pesquisadores sociais preocupados com a atuação prática. São também as mais solicitadas por organizações como instituições educacionais,
> empresas comerciais, partidos políticos etc. (Antonio Carlos Gil 2002, p. 42).

De acordo com Gil (2002) As pesquisas descritivas têm como objetivo principal descrever as características de uma determinada população ou fenômeno, proporcionando uma visão detalhada e compreensiva. Além disso, buscam estabelecer relações entre variáveis, ajudando a identificar padrões e tendências. Essas pesquisas são fundamentais para a formação de uma base sólida de conhecimento e para a compreensão aprofundada dos temas investigados

4 PREPARAÇÃO E RESULTADOS

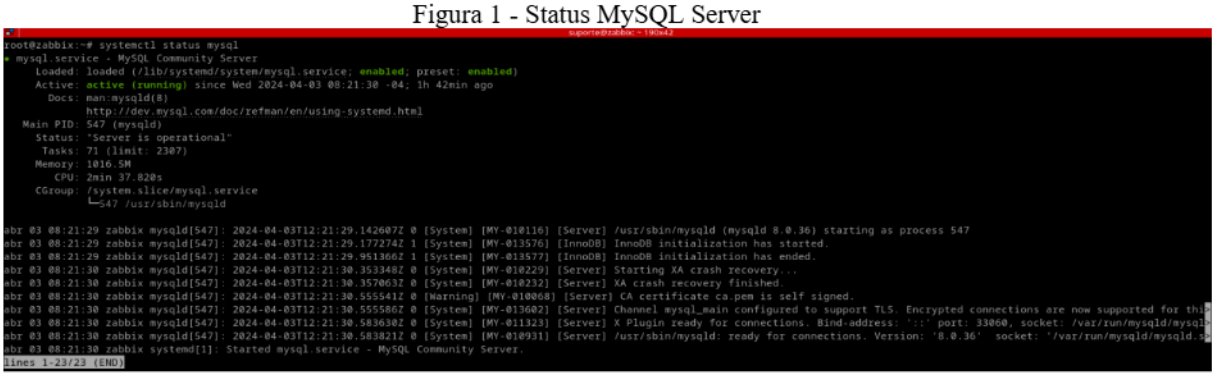
4.1 CONFIGURAÇÃO ZABBIX SERVER

No projeto foi instalado Zabbix Server em modo All in One (Tudo em Um), em uma Máquina e do tipo VM utilizando o Virtualbox, com sistema operacional Debian12, instalado com o Banco de Dados MySQL Server e em seguida instalando o Zabbix Server

no modo Pacotes com a versão 6.0 do zabbix, também foram instalados via pacotes o apache e agente do zabbix todos baixados direto do site do zabbix e instalando na VM Debian 12.

Para realizar a instalação do Zabbix Server se faz necessário já ter instalado o banco de dados, isto porque o Zabbix necessita para realizar o armazenamento dos dados coletados do itens e hosts monitorados.

Figura 1 - Status MySQL Server



Fonte: Próprio autor

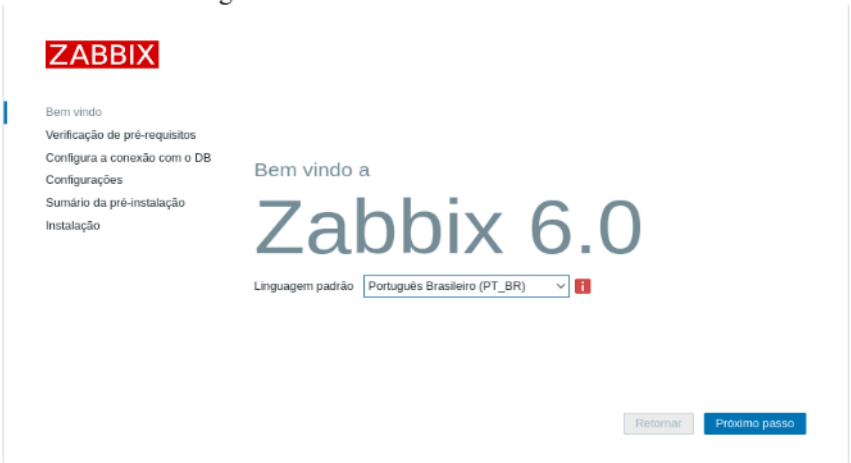
Para realizar a instalação do Zabbix Server é importante que as buscas sejam feitas no site Oficial do Zabbix, por onde é possível instalar o repositório com comando wget seguido do link de repositório, onde são buscados os pacotes zabbix no repositório para serem instalados no Sistema Debian12.

Para iniciar as configurações do Frontend do Zabbix Server, é necessário verificar o endereço IP a ser acessado no navegador de preferência, seguido de '/zabbix', por exemplo, '192.168.1.100/zabbix'. Se todas as configurações estiverem corretas, será exibida uma tela de boas-vindas do Zabbix.

Neste ponto, o usuário é convidado a selecionar um idioma de preferência para continuar com a instalação. Essa escolha é crucial para garantir que a interface do usuário seja apresentada no idioma desejado, facilitando a compreensão e a navegação durante o processo de configuração, mas o usuário pode também realizar alteração tanto do idioma quanto da cor do painel do Front-end caso queira, após realizadas as configurações.

Após a seleção do idioma, o processo de instalação prossegue, guiando o usuário por meio de etapas adicionais, como configuração inicial do banco de dados, definição de parâmetros de conexão e outras opções de personalização.

Figura 2 - Tela Boas Vindas Zabbix



Fonte: Próprio autor

Neste são feitas algumas verificações de pré-requisitos de banco de dado com o frontend. Um dos passos importantes na configuração de conexão com Banco de Dados é verificar a senha que foi criada com usuário zabbix, caso não lembre faça alteração na senha do usuário com o root MySQL. Finalizadas as configurações, segue-se à tela de login, que será oferecido para seu primeiro acesso à interface Web do Zabbix. Por padrão é feito com o usuário Admin e senha 'zabbix', após isso pode-se criar os primeiros usuários para configuração e administração do servidor Zabbix Server.

Figura 3 - Tela de Login

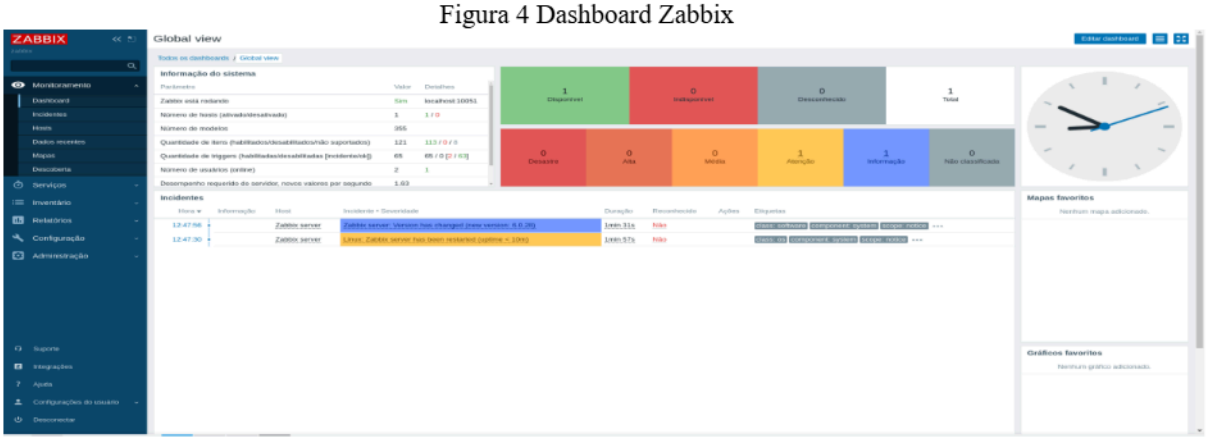
Fonte: Próprio autor

O zabbix utiliza uma ferramenta de segurança, na qual se o usuário errar a senha de acesso ao Front End, no próximo login bem sucedido, o zabbix mostrará a quantidades de tentativas mal sucedidas com IP que tentou realizar o acesso, com hora e data em que foram feitas as tentativas, e caso erre a senha por cinco vezes seguidas será feito um bloqueio por um período de 30 segundos, isto é usado como forma de mitigar tentativas de hacker por dicionário e força bruta.

Além disso, ao acessar a interface web do Zabbix Server, após o login, o

administrador terá à disposição muitos recursos. Os menus laterais fornecem acesso rápido às diversas áreas de configuração e administração do sistema, ao selecionar uma das opções, os submenus serão expandidos, revelando mais opções de configurações com detalhes de gerenciamento. Ainda no dashboard uma interface que exibirá um painel dinâmico, oferecendo uma visão geral dos alertas de hosts configurados. Essas informações são apresentadas de forma clara e organizada, permitindo aos administradores monitorar o status dos hosts e responder rapidamente a quaisquer problemas ou irregularidades detectadas pelo sistema. Podendo ser personalizados a exibição de dados, escolhendo quais widgets e métricas ou gráficos deseja visualizar com base nas necessidades de monitoramento..

Figura 4 Dashboard Zabbix



Fonte: Próprio autor

4.2 MONITORAMENTO DE HOSTS

Para realizar o monitoramento de um determinado equipamento de informática, inicialmente se faz necessário realizar o acesso ao equipamento a ser monitorado, fazer o download e instalação de um agente zabbix ou snmp para um monitoramento mais detalhado, realizar as devidas configurações neste agente instalado no equipamento alvo, informando para o gente os dados do servidor zabbix server. Após isso retorna ao servidor Zabbix Server faz o cadastramento do host e configurações de Itens e suas devidas triggers ou em um monitoramento simples somente o cadastro do host no zabbix server informando o ip do equipamento alvo do monitoramento.

4.3 MONITORAMENTO DE HOST SIMPLES

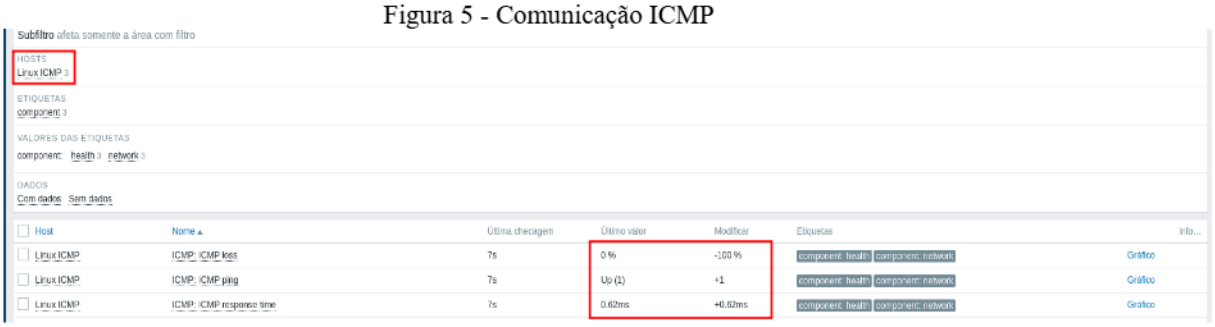
No monitoramento de Host Simples é utilizada a verificação do status de disponibilidade dos hosts em uma rede através do Protocolo ICMP. O Zabbix Server envia

solicitações de ping (ICMP) para os hosts monitorados, se um host responder ao ping, ele é considerado como "ativo" e "disponível". Se o host não responder aos pings dentro de um intervalo de tempo especificado, ele é marcado como "indisponível" e gera um alerta na interface de monitoramento.

Realizando testes com a criação de um Host no Servidor Server Zabbix para monitorar uma VM com sistema Debian instalado, para verificação com ICMP, onde no cadastramento foi escolhido o Template ICMP ping que traz Triggers que realizam os testes de perda de pacotes com ICMP loss, testes de conectividade como ICMP ping e testes de latência com ICMP response time.

Na figura-05 abaixo é mostrada a comunicação entre o Host Linux ICMP e Servidor Zabbix onde ICMP loss mostra que não está tendo perdas de pacotes (-100%) de pacotes até porque estão diretamente conectados, no ICMP ping , traz um resultado de Up (1) que mostra que tem conectividade entre os dispositivos.

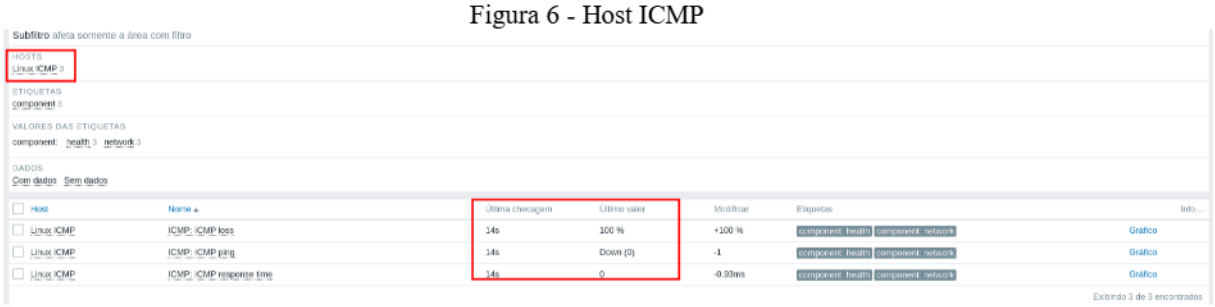
Figura 5 - Comunicação ICMP



Fonte: Próprio autor

Ao desligar o Host Linux ICMP, vai mostrar o contrário veja na figura-06 abaixo, com perdas de pacotes e resultado de Down (0) no ICMP ping, mostrando que não está tendo conectividade entre o equipamento e Servidor. Esse cenário indica claramente um problema de comunicação, o que pode ser um sinal de falha no hardware ou na configuração da rede. Em um caso real, o administrador já pode verificar o que está acontecendo. Ele poderia analisar os logs do sistema para identificar possíveis causas ou realizar testes adicionais de conectividade. Caso necessário, o administrador poderia ir até o host para fazer uma verificação no equipamento e resolver o problema rapidamente.

Figura 6 - Host ICMP



Fonte: Próprio autor

Visualizando o dashboard pode ser verificado que foi disparado a Trigger alertando um incidente onde não estava tendo comunicação entre o equipamento Linux ICMP e o Servidor Zabbix Server, pode se observar que o equipamento teve algumas falhas e foi reestabelecido e ainda mostra que está parado há 5 minutos. Este incidente sairá da dashboard assim que tiver comunicação entre o host Linux ICMP e o servidor Zabbix.

Figura 7 - Trigger de falhas ICMP

Fonte: Próprio autor

4.4 MONITORAMENTO DE HOST VIA AGENT ZABBIX

Agente Zabbix - é um software que pode ser instalado no host que se deseja monitorar. Ele faz coleta de várias informações do sistema, como uso da CPU, memória, utilização de disco, entre outras, e depois faz o envio para o servidor Zabbix Server. O Zabbix Server por sua vez recebe os dados coletados pelo Agente Zabbix, armazena esses dados em um banco de dados, após isso realiza os cálculos e se caso estes dados estiverem fora do padrões estabelecidos nas triggers, serão disparados alertas fornecendo as informações na interface web do Zabbix Server para que os administradores do sistema tomem as devidas providências com os incidentes que estiverem ocorrendo. O agente Zabbix é instalado no dispositivo alvo da monitoração. Possui capacidade de monitorar ativamente os recursos e aplicações locais (discos e partições, memória, estatísticas do processador, etc) (Zabbix Sia, 2024).

Após realizar o download do Agent Zabbix no host é necessário realizar a configuração do arquivo "zabbix_agentd.conf" que fica localizado dentro do diretório "zabbix". É importante nesta etapa observar o nome do host cadastrado no Servidor Zabbix para ser adicionado neste arquivo "zabbix_agentd.conf" que tem que ser igual ao nome que está configurado no servidor, também é neste arquivo que é adicionado o ip ou nome de domínio do Servidor Zabbix Server, para que o Agent Zabbix se comunique com o servidor informando os dados de coleta.

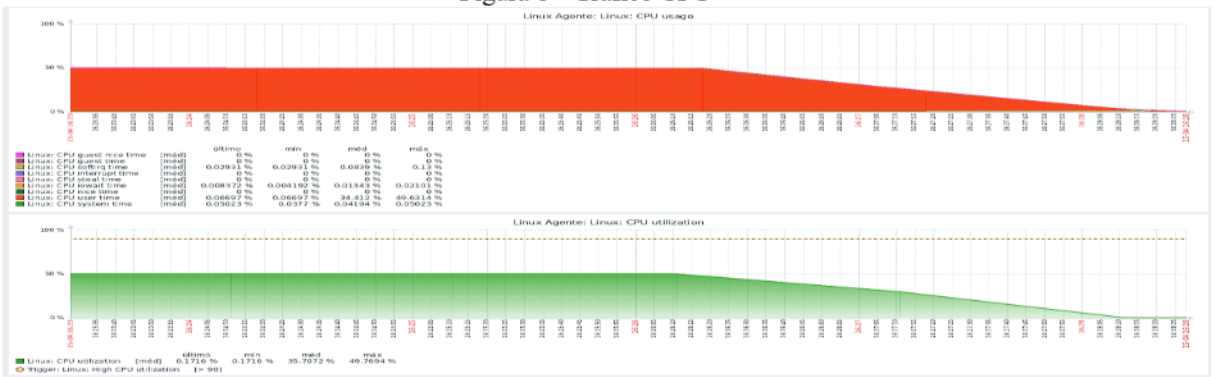
Após isso, no servidor Zabbix Server foi criado um host de nome Linux_Agente e adicionado ao grupo Linux que possui vários itens para realizar a verificação do sistema e em caso de problemas, as Triggers são disparadas, informando no dashboard o tipo de incidente.

Na VM linux foi utilizado uma ferramenta (stress-ng) que simula a carga em vários subsistemas computacionais, como CPU, memória e disco, com o objetivo de testar a estabilidade, o desempenho ou resistência do sistema sob condições de carga extrema.

> stress-ng - é uma ferramenta para carregar e estressar um sistema de computador que testará o estresse de um sistema de computador de várias maneiras selecionáveis. Ele foi projetado para executar vários subsistemas físicos de um computador, bem como os vários sistemas operacionais que têm interfaces do kernel do sistema (Manuais Ubuntu 2024)

Após toda configuração da VM e do servidor, foi possível observar que o servidor Zabbix Server estava realizando coleta dos dados da VM Linux_Agente como mostrado na figura-08 abaixo os respectivos dados coletados de CPU.

Figura 8 - Gráfico CPU



Fonte: Próprio autor

Também foi possível verificar, conforme a figura-09 a utilização de CPU e memória, pois foi disparado a Trigger informando ao usuário administrador que a VM Linux_Agente que estava com uma sobrecarga na CPU e na memória. Se o equipamento parar de funcionar,

também será disparada a trigger informando o problema com o equipamento. Numa notificação como esta, o administrador pode agir rapidamente para redistribuir a carga de trabalho ou ajustar os recursos alocados à VM. Além disso, ele pode investigar possíveis causas da sobrecarga, como processos em loop ou aplicações consumindo muitos recursos. Em casos extremos, um reinício controlado da VM ou apenas dos serviços pode ser necessário para restaurar o desempenho adequado.

Figura 9 - Alerta Agent-Zabbix

Fonte: Próprio autor

4.5 MONITORAMENTO DE HOST VIA SNMP

com relação ao monitoramento de host por SNMP no Zabbix Server, o protocolo SNMP é utilizado para monitorar dispositivos de rede, como roteadores, switches, impressoras entre outros equipamentos de infraestrutura de redes, o Zabbix Server realiza consultas SNMP aos dispositivos para coletar informações sobre seu status e desempenho. Em alguns equipamentos já possuem o snmp instalado como um padrão dos fabricantes, em outros como um servidor linux ou windows por exemplo é possível realizar a instalação e configuração do mesmo. Na figura-10 abaixo foi utilizado o comando snmpwalk e pode ser observado as OIDs de memória, cpu e de estado de link da interface na árvore MIB SNMP.

Figura 10 - OID MIBs

```
[root@localhost ~]# snmpwalk -On -v2c -c public 10.[redacted]124 | grep -m 3 memory
.1.3.6.1.2.1.25.2.3.1.3.1 = STRING: Physical memory
.1.3.6.1.2.1.25.2.3.1.3.3 = STRING: Virtual memory
.1.3.6.1.2.1.25.2.3.1.3.7 = STRING: Cached memory
[root@localhost ~]# snmpwalk -On -v2c -c public 10.[redacted]124 | grep -m 3 cpu
.1.3.6.1.2.1.25.4.2.1.2.10 = STRING: "mm_percpu_wq"
.1.3.6.1.2.1.25.4.2.1.2.21 = STRING: "cpuhp/0"
.1.3.6.1.2.1.25.4.2.1.2.22 = STRING: "cpuhp/1"
[root@localhost ~]# snmpwalk -On -v2c -c public 10.[redacted].124 | grep linkUP
.1.3.6.1.2.1.25.4.2.1.5.3094 = STRING: "--color=auto linkUP"
[root@localhost ~]#
```

Fonte: Próprio autor

4.6 NO MONITORAMENTO DA VM CENTOS SNMP

No monitoramento da Vm CentOS_SNMP foi instalado o protocolo snmp e configurados os arquivos snmptrapd.conf na vm para que esta realize comunicação com o servidor e no servidor foi configurado o arquivo "zabbix_server.conf". Este arquivo contém as configurações que definem como o Zabbix Server opera e se comunica com os agentes para realização das coletas de dados.

Na interface Zabbix Server foi criado um host e associado ao Templates para monitoramento de Memória, CPU, e Disco (HD). Na opção grupos, foram adicionados os grupos Discovery hosts e Linux, também foi escolhido o SNMP para monitoramento.

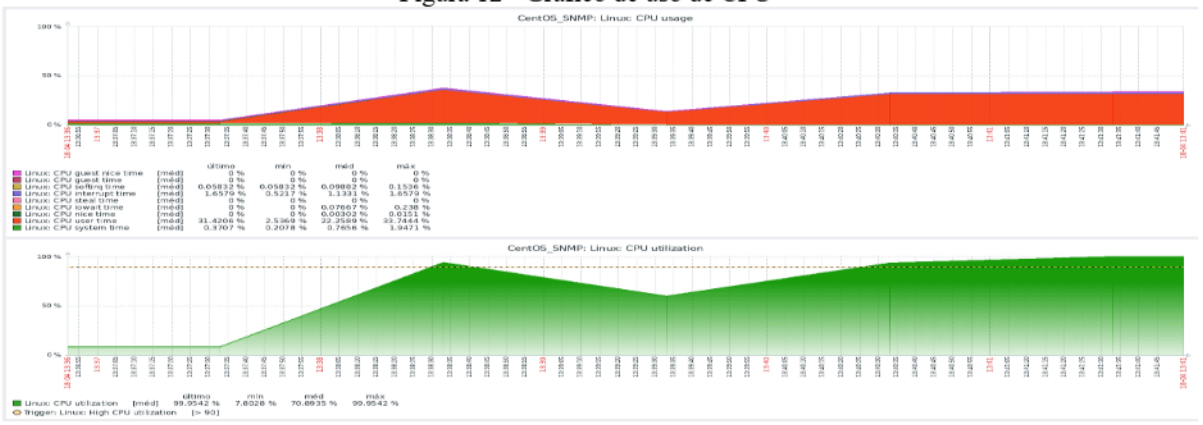
Em uma simulação forçando os trabalhos da CPU e Memória foi possível verificar que foram disparadas as Triggers informando que a vm CentOS_SNMP estava com problemas.

Figura 11 - Alerta CPUs SNMP

Fonte: Próprio autor

Também foi possível observar a coleta de vários dados da VM como cpu e hd nas figuras-12/13, Nos gráficos que possibilitaram ver com detalhes a quantidade de carga e como estava o funcionamento de cada Item. O administrador pode tomar uma decisão de imediato e resolver o problema antes que os usuários reclamem de uma lentidão ou de uma possível paralisação do sistema. Além disso, esses dados permitem identificar padrões de uso e antecipar problemas futuros. Com essa análise detalhada, o administrador consegue otimizar o desempenho dos sistemas e garantir uma operação mais eficiente. Dessa forma, a continuidade dos serviços é assegurada, minimizando impactos negativos para os usuários.

Figura 12 - Gráfico de uso de CPU



Fonte: Próprio autor

Figura 13 - Gráfico de uso de Disco

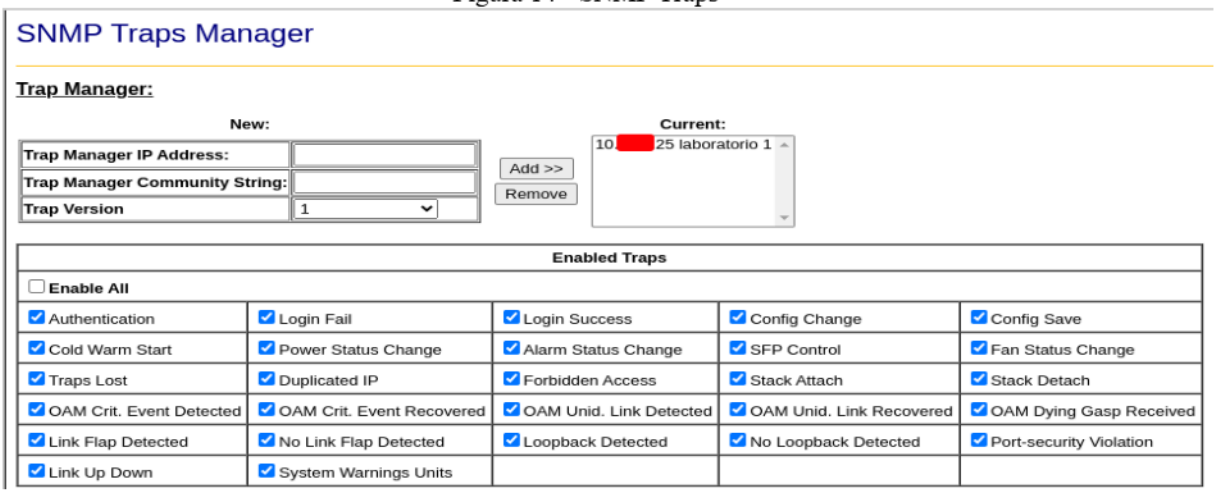
Fonte: Próprio autor

4.7 MONITORAMENTO DE SWITCH POR SNMP

Foi realizada a configuração de um host com nome *Switch Lab* para monitoramento no zabbix server, no Template foi escolhido o *Network Generic Device by SNMP*, que traz 12 Itens de monitoramento e 6 Triggers para serem disparadas informando problemas quando o Switch estiver com funcionamento fora dos padrões estabelecidos. O switch já estava com o protocolo SNMP instalado, no qual foi configurado *SNMP Traps Manager* com IP do Servidor Zabbix Server e a Comunidade (laboratório).

> Modelos de templates permitem agrupar itens, gatilhos e outras entidades úteis de forma que possam ser reutilizados continuamente pela aplicação aos hosts em uma única etapa. Quando um modelo é associado a um host, o host herda todas as entidades do modelo. Então, basicamente um monte de verificações podem ser aplicadas muito rapidamente (Zabbix Sia, 2024).

Figura 14 - SNMP Traps



Fonte: Próprio autor

Após as configurações realizadas foi possível verificar que o Servidor Zabbix Server estava realizando a coleta de várias informações do switch incluindo o uso de memória , utilização de CPUs e status de interfaces. Também foi possível verificar que após um tempo com a interface desligada a Trigger disparou informando que havia portas do switch com status de Link Down.

Figura 15 - Alerta Switch SNMP

Fonte: Próprio autor

5 CONSIDERAÇÕES FINAIS

Neste trabalho apresentamos a implementação do Zabbix Server para o monitoramento de rede, utilizando alguns métodos de coleta de dados, incluindo ICMP, SNMP e o agente Zabbix. O objetivo principal foi aplicar o que aprendemos e melhorar nosso conhecimento através da implementação de um servidor, mesmo que em VM Zabbix simulando um ambiente real, mas que seria de grande importância para nosso aprendizado e uma valiosa experiência de certa forma realizar o gerenciamento de uma infraestrutura de

rede.

A coleta de dados através do ICMP permitiu uma verificação simples, porém fundamental, da disponibilidade dos dispositivos de rede. A utilização do SNMP possibilitou uma monitorização mais detalhada, permitindo o acompanhamento de métricas como tráfego de rede, uso de CPU e utilização de memória. Por fim, o uso do agente Zabbix proporcionou uma visão completa do desempenho dos servidores e sistemas locais, permitindo monitorar aspectos específicos do sistema operacional e aplicativos.

Ao longo da implementação, alguns desafios foram enfrentados, como a configuração inicial dos dispositivos para responder às consultas SNMP e a otimização dos parâmetros de coleta de dados para garantir um equilíbrio entre precisão e carga de processamento, como por exemplo como encontrar o OID da MIB correspondente ao processador ou memória. No entanto, esses obstáculos foram superados com sucesso, durante a pesquisa, além de descobrirmos que o Zabbix já traz muitos Temples com os mais variados Itens de coleta, podendo no próprio zabbix realizar o monitoramento customizado, mas que a pesquisas e estudo do protocolo SNMP contribuíram para uma compreensão mais profunda no monitoramento de rede.

Embora este estudo tenha alcançado seus objetivos propostos, reconhecemos algumas limitações. Por exemplo, a análise de dados foi realizada em um ambiente de teste controlado utilizando VMs, e os resultados podem variar em ambientes reais de produção mais complexos. Além disso, a implementação do Zabbix Server foi focada principalmente no monitoramento de infraestrutura de rede, deixando espaço para investigações futuras sobre monitoramento de aplicativos e serviços específicos.

Desta forma, o resultado do trabalho foi alcançado, além de uma oportunidade muito importante para aplicar os conhecimentos adquiridos na faculdade.

REFERÊNCIAS

FOROUZAN, Behrouz A. Comunicação de dados e redes de computadores. 4. ed. AMGH, 2010.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.

LIMA, Janssen dos Reis. Monitoramento com ZABBIX. 2. ed. São Paulo: Novatec, 2020.

KUROSE, James F. Redes de computadores e a internet: uma abordagem top down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

TANENBAUM, Andrew S. Redes de computadores. 4ª Edição, Editora Campus Rio de Janeiro , 2003.

UBUNTU. stress-ng(1) manual page. Disponível em: <https://manpages.ubuntu.com/manpages/jammy/en/man1/stress-ng.1.html>. Acesso em: 23 ago. 2024.

ZABBIX DOCUMENTATION. (2021). Zabbix Manual. Disponível em: <https://www.zabbix.com/documentation/5.2/manual/discovery> . Acesso em: 23 ago. 2023.