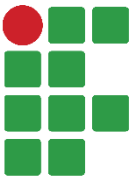


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES
CAMPUS MACAPÁ

ISABELLY COSTA DE ABREU
KAYUÃ KAYO MARIANO RODRIGUES BARBOSA

ESTUDO DE CASO NO SESI SENAI DR - AP: Implementação da ferramenta Zabbix na versão 6.0 LTS para monitoramento dos equipamentos de rede.

MACAPÁ - AP
2022

ISABELLY COSTA DE ABREU
KAYUÃ KAYO MARIANO RODRIGUES BARBOSA

ESTUDO DE CASO NO SESI SENAI DR - AP: Implementação da ferramenta Zabbix na versão 6.0 LTS para monitoramento dos equipamentos de rede.

Trabalho de Conclusão de Curso apresentado a coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção de título de Tecnologia em Redes de Computadores.
Orientador: Me. Thiego Maciel Nunes

MACAPÁ - AP
2022

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

A162e Abreu, Isabelly Costa
Estudo de caso no sesi senai dr - ap: Implementação da ferramenta Zabbix na versão 6.0 LTS para monitoramento dos equipamentos de rede. / Isabelly Costa Abreu, Kayuã Kayo Mariano Rodrigues Barbosa. - Macapá, 2022.
62 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2022.

Orientador: Me.Thiêgo Maciel Nunes.

1. Monitoramento. 2. Gerenciamento em rede. 3. Zabbix. I. Barbosa, Kayuã Kayo Mariano Rodrigues. I. Nunes, Me.Thiêgo Maciel , orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

ISABELLY COSTA DE ABREU
KAYUÃ KAYO MARIANO RODRIGUES BARBOSA

ESTUDO DE CASO NO SESI SENAI DR - AP: Implementação da ferramenta Zabbix na versão 6.0 LTS para monitoramento dos equipamentos de rede

Trabalho de Conclusão de Curso apresentado a coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção de título de Tecnologia em Redes de Computadores.
Orientador: Me. Thiego Maciel Nunes

BANCA EXAMINADORA

Thiêgo Maciel Nunes
Prof. Me. Thiêgo Maciel Nunes (Orientador)
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Prof. Me. Jairo de Kassio Siqueira Barreto
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Klenilmar Lopes Dias
Prof. Me. Klenilmar Lopes Dias
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Aprovado em: 23/11/2022

Conceito/Nota: 95

RESUMO

Atualmente, conforme uma empresa cresce, a infraestrutura de rede deve acompanhar esse processo a fim de realizar a entrega dos serviços internos nesses novos departamentos. Dessa forma, acarretando no aumento do número de equipamentos em rede para as atividades de diversos departamentos, houve a necessidade de monitorá-los. A gerência constitui um conjunto de processos para monitorar a rede, a fim de deixá-la eficiente e torná-la tolerante a falhas. Com vários ativos, uma falha pode acarretar indisponibilidade no ambiente computacional, paralisando as atividades. Por isso, esse trabalho tem como objetivo apresentar um estudo de caso sobre a implementação da ferramenta Zabbix para o monitoramento e gerenciamento dos equipamentos na rede da empresa SESI SENAI DR - AP. O Zabbix é uma solução capaz de monitorar a rede de computadores, permitir a visualização dos equipamentos através da interface web e emitir alertas sobre eventualidades. O trabalho foi desenvolvido com base em pesquisas bibliográficas para embasamento teórico, pesquisa experimental para o procedimento de implementação, método dedutivo para constatar os testes e o método qualitativo para analisar as informações coletadas. Por fim, a implementação do serviço Zabbix demonstrou que a utilização da ferramenta é essencial para o parque computacional do SESI SENAI DR - AP, por ser capaz de facilitar o monitoramento dos equipamentos de rede e de enviar alertas aos responsáveis pelo ambiente computacional sobre ocorrências prejudiciais, o Zabbix colaborou com a melhora do gerenciamento da rede de computadores da empresa.

Palavras-Chave: monitoramento; gerenciamento em rede; zabbix.

ABSTRACT

Currently, as a company grows, the network infrastructure must accompany this process in order to carry out the delivery of internal services in these new departments. Thus, resulting in an increase in the number of networked equipment for the activities of various departments, there was a need to monitor them. Management constitutes a set of processes to monitor the network in order to make it efficient and fault-tolerant. With several active components, a defect can cause unavailability in the computing environment, paralyzing activities. Therefore, this work aims to present a case study on the implementation of the Zabbix tool for monitoring and managing assets in the network of the company SESI SENAI DR - AP. Zabbix is a solution capable of monitoring the computer network, allowing the visualization of equipment through the web interface and issuing alerts on eventualities. The work was developed based on bibliographical research for theoretical basis, experimental research for the implementation procedure, deductive method to verify the tests and the qualitative method to analyze the collected information. Finally, the implementation of the Zabbix service demonstrated that the use of the tool is essential for the SESI SENAI DR - AP computing park, as it is able to facilitate the monitoring of network equipment and send alerts to those responsible for the computing environment about harmful occurrences, the Zabbix helped to improve the management of the company's computer network.

Keywords**:** monitoring; network Management; zabbix

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AP	Amapá
CFP	Centros de Formação Profissional
CPD	Centro de Processamento de Dados
CPU	Unidade Central de Processamento
DHCP	Protocolo de Configuração Dinâmica de Hosts
DNS	Sistema de Nome de Domínio
DR	Departamento Regional
DVR	Gravador de Vídeo Digital
FCAPS	Falha; Configuração; Contabilização; Gerenciamento e Segurança
GB	Gigabyte
GUI	Interface Gráfica do Usuário
IP	Protocolo de Internet
ISO	Organização Internacional para Padronização
LTS	Suporte de Longo Prazo
MIB	Base de informações de gerenciamento
RAM	Memória de Acesso Aleatório
SENAI	Serviço Nacional de Aprendizagem Industrial
SESI	Serviço Social da Indústria
SGBD	Sistema de Gerenciamento de Banco de Dados
SLA	Acordo de Nível de Serviço
SMS	Serviço de Mensagens Curtas
SNMP	Protocolo Simples de Gerenciamento de Redes
SSI	Saúde e Segurança na Indústria
TI	Tecnologia da Informação
TMN	Gerenciamento de Rede de Telecomunicações
VM	Máquina Virtual

SUMÁRIO

1 INTRODUÇÃO

Há tempos, nota-se cada vez mais o aumento de computadores devido aos recursos oferecidos por eles e a presença de mecanismos para gerenciar essa grande quantidade de máquinas em uma rede. Para Forouzan (2010), uma rede de grandes proporções é formada por vários equipamentos ligados entre si de forma física ou lógica e com atividades acontecendo a todo instante.

Com vários componentes de comunicação ativos, uma falha pode causar instabilidade em todo sistema de comunicação e por isso exige-se uma gerência de rede para manter estáveis o funcionamento das máquinas e manter sob controle os componentes, a fim de maximizar o desempenho de cada dispositivo (STORCH, 2008). Como consequência, empresas de *software* oferecem uma ampla gama de ferramentas que facilitam a gerência de equipamentos, tanto em médias quanto em grandes empresas, independentemente do tamanho da rede, permitindo que diferentes setores automatizem os processos de monitoramento (FERNANDES, 2021).

Dentre esses softwares, de acordo com os estudos realizados por sites[1] e artigos[2] voltados ao conteúdo de tecnologia da informação e monitoramento de rede, a ferramenta Zabbix vem constantemente aparecendo dentro dessas pesquisas listando-o como uma das melhores ferramentas para o monitoramento de rede, principalmente por ser *Open Source* e com nenhum custo para implementação da ferramenta e *upgrades* posteriores, a ferramenta tem uma grande comunidade e manuais disponíveis para ajudar o usuário a entender a ferramenta (CAPTERRA, 2020).

Tendo em vista os aspectos observados, destaca-se como objetivo deste trabalho implementar e demonstrar o funcionamento do *software* de gestão *Zabbix* ao fazer o monitoramento e gerenciamento dos sistemas de rede no SESI SENAI DR - AP, promovendo maior visibilidade dos dados obtidos através de *dashboard* disponíveis no *front-end* do *Zabbix*, além de colaborar com a gestão e a segurança no ambiente para evitar futuros imprevistos na rede.

---

[1] Capterra, Monitoramento de rede. Disponível em: <https://www.capterra.com.br/blog/1583/monitoramento-de-rede>. Acessado em 23 de Nov. 2022; Netsupport, Monitoramento de rede. Disponível em: <https://netsupport.com.br/monitoramento-de-rede/>. Acessado em 23 de Nov. 2022; Network, K. N. Monitoramento de rede. Disponível em:<https://network-king.net/pt-pt/ferramentas-de-monitoramento-de-rede/>. Acessado em 23 de Nov. 2022.

[2] Santos, M. A. B; Barros, R. C. Direções no monitoramento em redes de larga escala: Uma visão geral, ferramentas e tendências. Disponível em: <https://www.editorarealize.com.br/editora/anais/conidis/2016/TRABALHO_EV064_MD1_SA6_ID2261_20102016121118.pdf>. Acessado em 23 de Nov. 2022; Scapin, A. H. Análise de ferramentas de gerência de redes e interfaces web. Disponível em: <https://www.ufsm.br/app/uploads/sites/495/2019/05/2015-Alex-Scapin.pdf>. Acessado em 24 de Nov. 2022.

Considerando o conjunto de computadores que formam a rede do SESI SENAI DR – AP, por envolverem vários serviços e empregarem muitas informações, tais como publicações de editais, serviços internos e até externos oferecidos à comunidade, entre outros, torna-se indispensável o monitoramento dos equipamentos de rede e a verificação do desempenho dos serviços que são entregues pela equipe de T.I para a continuidade dessas atividades.

Destaca-se como problemática neste trabalho a indisponibilidade de conexão e falhas que ocorrem na rede, fatores responsáveis pela paralisação dos equipamentos que compõem a rede da empresa e demais serviços, podendo paralisar parcial ou totalmente as atividades desenvolvidas. Segundo Kurose (2013), sobre o gerenciamento de falhas, destaca que o profissional precisa detectar, registrar e entender anomalias que podem afetar qualquer conjunto de serviço ou atividade e utilizar seu conhecimento para determinar como resolvê-lo.

As principais falhas recorrentes na rede de computadores podem ser identificadas através de falha de *hardware*, erro de configuração, *software* ou falha em enlaces de dados. Conforme explica Tanenbaum e Wetherall (2011), a rede e os equipamentos têm de ser à prova de falhas quando este estiver em operação, logo nota-se que é indispensável a utilização de ferramentas para supervisionar o desempenho da rede e emitir relatórios caso algum componente apresente indisponibilidade.

Desse modo, faz-se necessário a implementação de um sistema de gerenciamento na rede que visa trazer respostas significativas e ágeis para os profissionais de T.I sobre possíveis imprevistos que possam ocorrer. De acordo com Júnior (1999, p.365), “Um sistema de gerenciamento de rede é composto por ferramentas para o monitoramento e controle da rede”. Sendo assim, foi aplicado neste trabalho conceitos de gerenciamento, abordando o uso do protocolo SNMP (*Simple Network Management Protocol*) e a execução da ferramenta *Zabbix* para gerenciar um conjunto de equipamentos no ambiente de redes, promovendo assim uma melhor visualização desses ativos via interface do *web Zabbix*.

O presente trabalho está organizado em seções, na seção 2 é apresentada a justificativa do trabalho, onde se retrata a motivação do estudo acerca do tema. Na seção 3 é apresentada a hipótese, nessa seção trata-se da resposta a problemática inserida na pesquisa. Na seção 4 são apresentados os objetivos do trabalho, onde se encontram os pontos essenciais a serem demonstrados no tema em questão. A seção 5 refere-se ao embasamento teórico que foi buscado para a formulação deste trabalho. Na seção 6 encontram-se os trabalhos relacionados. No 7 aborda a metodologia utilizada. Na seção 8 é apresentado o estudo de caso, parte principal do trabalho. Na seção 9 está a conclusão e trabalhos futuros e na seção 10 encontram-se as referências utilizadas em todo o trabalho.

2 JUSTIFICATIVA

Baseia-se este estudo na resposta à problemática de eventuais falhas ocorridas na infraestrutura de rede que podem acarretar em indisponibilidade de conexão, falha em equipamentos, perda de equipamentos, entre outros, resultando em falhas na entrega de serviços disponibilizados pela rede do SESI SENAI DR – AP.

Com base em estudos no portal Teleco (2012) tendo em vista o aumento da dependência das redes, negligenciar a gerência dos equipamentos de rede e aplicações que fornecem serviços críticos, podem acarretar em prejuízos econômicos às empresas. Sendo assim, o gerente da rede deve ter a capacidade de identificar os gargalos, falhas, problemas de segurança e conseguir avaliar o desempenho dos equipamentos, servidores e serviços prestados pela equipe de T.I de modo a visualizar possíveis atualizações na rede para atender da melhor forma a necessidade do usuário.

Corroborando com o crescimento das redes, conforme o *Annual internet report* 2018 - 2023 da cisco (relatório anual da Internet da Cisco de 2018 até perspectivas de 2023) onde mostra uma análise do cenário global que avalia a transformação digital em vários segmentos de negócios e aborda previsões, com base nas análises, para o ano de 2023 (CISCO, 2020). Um dado importante para este trabalho é a análise de conexões e dispositivos onde a previsão afirma que para 2023 o número de dispositivos conectados a redes IP será mais de três vezes a população global. Com base nessa análise Cisco (2020, p. 1) “Haverá 3,6 dispositivos em rede por pessoa até 2023, acima dos 2,4 dispositivos em rede per capita em 2018. Haverá 29,3 bilhões de dispositivos em rede até 2023, contra 18,4 bilhões em 2018”. E em uma pesquisa mais focalizada na região da América Latina (LATAM), Cisco (2020, p.3) “Até 2023, a LATAM terá 2,1 bilhões de dispositivos/conexões em rede, contra 1,4 bilhão em 2018.”

A partir do crescimento de uma rede de computadores, ela se torna cada vez mais complexa, com mais conectividades, enlaces, equipamentos e serviços entregues. Junto a isso, vem a importância da adoção de uma ferramenta de monitoramento para um melhor gerenciamento e manuseio dos equipamentos, servidores e enlace de dados, colaborando na rapidez de resposta aos problemas ocorridos. (OTAVIO; CÉSAR; NATIVIDADE, 2013).

Diante do exposto, através da solução facilitadora *Zabbix*, é possível monitorar vários parâmetros dos dispositivos e de servidores na rede do SESI SENAI DR - AP, de modo a visualizar possíveis problemas ocorridos através de gráficos, *dashboard* de dados e mecanismos de notificações com a possibilidade de configurar alertas para praticamente qualquer evento, proporcionando a rápida reação aos problemas apresentados na rede (Zabbix, 2022).

3 HIPÓTESE

Este sistema de monitoramento irá colaborar com a identificação dos dispositivos de rede de computadores do SESI SENAI DR - AP e trará benefícios significativos com o mapeamento visual, por meios de mapas e *dashboards*, identificando e relatando problemas ocorridos nesses equipamentos.

4 OBJETIVOS

4.1 Objetivo geral

Implementar a solução *Zabbix* para monitoramento e gerenciamento dos equipamentos da infraestrutura de rede do SESI SENAI DR – AP, buscando mapear e catalogar *Switches*, DVR's, máquinas virtuais, enlaces da empresa e ter resposta ativa em resoluções de problemas ocorridos nos equipamentos da rede de computadores.

4.2 Objetivo específico

- Instalar o serviço Zabbix em uma arquitetura de 3 camadas.
- Realizar a exportação do banco de dados do Zabbix da versão antiga e importar esse mesmo banco de dados na arquitetura nova.
- Habilitar o protocolo SNMP nos equipamentos que serão gerenciados e monitorados pelo *Zabbix*, e nas máquinas virtuais, instalar o agente *Zabbix* para o monitoramento.
- Criar *Dashboards* e mapas para visualização das ocorrências nos *Switches*, DVR, máquinas virtuais e enlace de dados.

5 FUNDAMENTAÇÃO TEÓRICA

Antes de abordar qualquer aspecto sobre a implementação da solução *Zabbix* na rede de computadores do SESI SENAI DR - AP, é necessário discorrer sobre os assuntos referente a esse objetivo.

Este tópico apresenta uma breve fundamentação teórica sobre as áreas envolvidas no desenvolvimento deste estudo, abordando questões referentes ao Protocolo SNMP, Agent SNMP, Gerenciamento e Monitoramento de Redes e a ferramenta em questão *Zabbix*.

5.1 Protocolo SNMP e Agent SNMP

De acordo com Ribeiro (2016), o protocolo SNMP (*Simple Network Management Protocol* ou Protocolo Simples de Gerenciamento de rede) é um protocolo desenvolvido para o gerenciamento de dispositivos em um ambiente de rede que possibilita recolher informações sobre os componentes que estão conectados a ela como roteadores, *bridges, switches* e os computadores ligados diretamente na rede.

Esse protocolo foi criado para facilitar o gerenciamento e o monitoramento nas redes, é descrito pela primeira vez na RFC 1067 em 1988 e possui atualmente três versões conhecidas como SNMPv1, SNMPv2 e SNMPv3. É hoje considerado um dos protocolos mais usados em ambientes de monitoramento, já que permite trabalhar com produtos e serviços de diversos fabricantes (ROCHA, 2017).

Para Kurose (2013, p. 563) “o SNMP é usado para transmitir informações e comandos entre uma entidade gerenciadora e um agente que os executa em nome da entidade dentro de um dispositivo de rede gerenciado”. A função básica do protocolo é proporcionar um gerenciamento simples que forneça dados de status ao administrador sobre os componentes monitorados como uso, nível de colisão, vazão, taxa de erros, entre outros itens solicitados.

Segundo Rocha (2017), o protocolo SNMP já vem embutido pelo fabricante, por isso não é possível instalá-lo e sim apenas habilitá-lo na máquina através de uma alteração de configuração. O protocolo permite ainda designar uma ou mais máquinas da rede como gerentes ou Agent SNMP, com isso fica possível administrar todo o sistema para facilitar a identificação de falhas na rede. Para isso, é comum que os administradores usem o *Management Information Base* (Base de informações de gerenciamento, ou MIB), uma árvore hierárquica organizada por tipo de informação, para que as informações necessárias para gestão de cada componente fiquem gravadas.

Uma estação gerenciadora, de acordo com Forouzan (2010) é denominada agente quando um roteador ou um dispositivo executa o programa-servidor SNMP. Da mesma forma, uma estação gerenciadora é denominada gerente quando um *host* roda o programa-cliente SNMP, assim o gerenciamento é obtido pela interação entre agente e gerente.

5.2 Gerenciamento e monitoramento de redes

A gerência é o meio pelo qual o administrador da rede utiliza um conjunto de ferramentas de monitoramento, normalmente composta por uma solução de *hardware* e *software*, capaz de acompanhar o funcionamento das máquinas, centralizar de forma mais efetiva as informações e gerar dados históricos sobre o ambiente computacional, com intuito de trabalhar de maneira mais assertiva em um momento de indisponibilidade de algum componente (BUENO, 2012).

Desta maneira, conforme expressa Saydam (1996), o gerenciamento em uma rede compreende o conjunto de oferta, integração e coordenação de componentes como *hardware*, *software* e profissionais responsáveis por monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede para atender as exigências operacionais, de performance e de qualidade aos serviços.

Para Forouzan (2010), pode ser definido como monitoramento dos sistemas, realização de testes, configurações e diagnósticos de componentes que atendem um conjunto de exigências estabelecidas de um determinado local. Dentre as exigências, são efetuadas operações estáveis e eficientes da rede para buscar oferecer sempre maior qualidade aos serviços prestados a um custo razoável.

O sistema de gerenciamento visa manter o bom desempenho das atividades em um nível admissível para a realização das atividades, mas para isso é necessário que o profissional de TI conheças certas informações como configuração, falhas, desempenho, segurança e contabilizações que podem ser utilizadas por uma solução, no qual verifique quais componentes funcionam, quais estão apresentando problemas e quais definitivamente não estão funcionando (KUROSE e ROSS, 2006).

5.2.1 Modelo FCAPS

Em suma, o modelo de gerenciamento serve para orientar e ajudar os gestores de redes a organizarem as informações coletadas dos equipamentos para fazer uma análise mais objetiva.

Para esse auxílio a ISO (*International Organization for Standardization*) desenvolveu o modelo FCAPS *(Fault, Configuration, Accounting, Performance and Security Management*) para auxiliar os profissionais de TI a obterem informações mais assertivas sobre a rede, apresentando estruturas conceituais de gerência de diferentes tarefas e funções (VARGAS, 2020).

Cada área do modelo FCAPS encaixa-se nas necessidades que comportam os equipamentos na rede e esse modelo de gerenciamento se tornou base para os demais por definir área funcionais de gerência de redes, como Detecção de Falhas e Correção; Configuração e Operação; Contabilização e Faturamento; Ajustes de Performance e Otimização; Garantia de Segurança e Proteção (COMER, 2008).

Com isso, a criação das 5 áreas de gerenciamento de redes estabelecida pela ISO tornou-se uma extensão do modelo de gestão de redes conhecido como *Telecommunication Management Network* (TMN), envolvendo o gerenciamento de falhas, gerenciamento de configuração, gerenciamento de contabilização de desempenho e gerenciamento de segurança. A seguir será abordado cada item deste modelo.

5.2.1.1 Gerenciamento de falhas (*Fault*)

Essa área do gerenciamento é mais comumente visível nos ambientes computacionais e possui foco principal neste trabalho, está dividida em monitoração, diagnóstico e envio de notificações aos administradores ou correção das falhas de forma automática. Segundo Simões (2010), para manter a rede funcional e sem falhas, a monitoração tem a função de evitar que complicações ocorram progressivamente, já o diagnóstico e o envio de notificações visam notificar sobre o funcionamento da rede e emitir alertas por meio de notificações, alarmes e representações gráficas sobre o estado dos componentes, caso ocorra falhas inesperadas na rede.

O contínuo monitoramento da rede serve para tratar sobre o funcionamento dos dispositivos para correção de problemas que envolvem as operações, detecção e reação às condições de falhas da rede. Em suma, a gerência de falhas se diferencia da gerência de desempenho por solicitar uma intervenção imediata a fim de evitar complicações no sistema e prejudicar o desenvolvimento das atividades, enquanto a desempenho adota uma abordagem de intervenção a longo prazo (DUARTE, 2011).

Nesse momento, o gerenciamento de falhas monitora, faz o diagnóstico e tenta resolver o elemento da rede que apresenta alguma falha, como cita (KUROSE & ROSS, 2010) é onde ocorre a identificação e a tomada de ação às condições adversas da rede. Durante o gerenciamento de falhas, para reagir rapidamente contra os incorreções e erros que surgem nos

dispositivos, as ferramentas de monitoramento, como o Zabbix, auxiliam para detectar onde está falhando e alertar o administrador sobre o local para isolar a área e reduzir os impactos e não afetar os demais computadores.

Segundo Stallings (2005), existe uma diferença entre o termo erro e falha, tendo em vista que a falha é uma condição anormal e exige uma ação de gerenciamento imediata para o contínuo desenvolvimento das atividades e origina-se pela excessiva quantidade de erros durante seu processamento em um sistema operacional ou em um *hardware*, enquanto que o erro é apenas um evento único e inesperado.

5.2.1.2 Gerenciamento de configuração (*Configuration*)

Esse tipo de gerenciamento permite ao administrador monitorar a configuração da rede e dos equipamentos que pertencem ao ambiente, como as configurações de *hardware* e *software*, proporcionando maior o gerenciamento e rastreio de diversos elementos (DUARTE, 2011). Por via de regra, esta tarefa comporta em um banco de dados informações sobre o sistema das máquinas.

O gerenciamento de configuração mantém as especificações dos equipamentos gerenciados com o registro e controle das alterações ocorridas nas configurações desses dispositivos, como também atua para realizar ajustes de configuração essenciais para a solução de problemas e para restabelecer ou melhorar a performance da rede (VARGAS, 2020).

Para Castro et al. (2013) “Esta configuração consiste em descobrir a rede, os dispositivos que fazem parte dela, a manutenção e o que deverá ser monitorado tanto logicamente quanto fisicamente”. Desse modo, a fim de auxiliar o administrador da rede, precisa-se que os dispositivos estejam devidamente configurados com intuito de detalhar o exercício das máquinas que fazem parte da rede e quais estão sendo monitorados de forma física e lógica.

5.2.1.3 Gerenciamento de Contabilização (*Accounting*)

O gerenciamento de contabilização engloba meios utilizando estatísticas para compreender melhor o tráfego da rede, através da coleta de dados e a análise da mesma. Como cita Vargas (2020), são coletadas informações sobre a aplicação dos processos da rede, a qual é possível utilizar para predeterminar métricas, analisar o resultado de um processo e determinar o custo das operações.

Esse recurso permite que o administrador coordene os meios a serem utilizados de maneira satisfatória pelos usuários, permitindo melhorar a distribuição conforme a capacidade de cada um. Desse modo, o gerenciamento de configuração visa minimizar os problemas com a organização da capacidade de distribuição, administrar a autorização de contas, permissões e ao mesmo tempo reunir informações sobre a estatística pelo serviço oferecido aos usuários, para aplicar os limites de cotas dos recursos (DUARTE, 2011).

Com esse gerenciamento, o administrador da rede controla os recursos disponibilizados para evitar que os usuários abusem de privilégios e que agravam os sistemas da rede, prejudicando assim as demais atividades. Visa também melhorar a eficácia da usabilidade por parte dos usuários, conhecer detalhadamente a rotina de atividades, a fim de planejar e acompanhar o crescimento da rede, podendo ser usado para dar suporte a auditorias e comunicações de fraudes a partir das análises feitas (CASTRO et al., 2013).

5.2.1.4 Gerenciamento de Desempenho (*Performance*)

De acordo com Vargas (2020), o gerenciamento de desempenho é responsável por garantir que rede mantenha o desempenho em níveis aceitáveis, empregando sistemas de rastreamento e estatísticas da rede para coletar os dados sobre a utilização dos enlaces e dos dispositivos, análise do tempo de resposta e informações de disponibilidade. Com esses dados é possível determinar tendências e resolver problemas relacionados ao funcionamento dos dispositivos.

A finalidade do gerenciamento de desempenho é mensurar as atividades dos computadores, informar aos responsáveis, verificar os resultados obtidos e monitorar o desempenho dos distintos componentes da rede (KUROSE, 2010). Entre os vários componentes que se encontram presentes na rede estão os dispositivos individuais, como roteadores, *switches*, enlaces, e as aplicações fim a fim, como um trajeto pela rede.

5.2.1.5 Gerenciamento de Segurança (Security)

Com o gerenciamento de segurança é possível controlar os acessos aos sistemas e recursos de rede de acordo com as políticas estabelecidas pelo ambiente, para realizar a prevenção de ataques e demais acontecimentos indesejáveis que são capazes de interferir no funcionamento da rede e prejudicar as atividades (DUARTE, 2011).

O gerenciamento de segurança visa prover facilidades para proteger os recursos e as informações da rede. Esse sistema regula e controlar o acesso aos serviços da rede e segmenta determinadas informações às pessoas autorizadas, o que inclui atividades como detecção, autenticação, autorização e registros de usuários as tentativas de acesso ao sistema, além de controlar principalmente o acesso aos roteadores, switches e equipamentos da rede (ABREU e PIRES, 2004).

Conforme explica Vargas (2020), a segurança é responsável por lidar com os direitos de acesso às pessoas autorizadas, como autenticação e autorização, privacidade de dados e auditoria de violações de segurança, com intuito de amenizar as vulnerabilidades da infraestrutura e gerenciar as possíveis ameaças.

5.3 Métricas para análise do gerenciamento

De acordo com as ferramentas de gerências para o ambiente de redes de computadores, há uma predominância na combinação de cinco elementos diferentes para fazer a medição do funcionamento e do desempenho, conhecidas como disponibilidade, tempo de respostas, utilização da rede, vazão e a capacidade de transmissão (ABREU e PIRES, 2004).

5.3.1 Disponibilidade

Para determinar se a rede está funcionando corretamente, é preciso verificar a disponibilidade dos sistemas, dos equipamentos, analisar o tráfego e verificar se os dados estão percorrendo na rede ou não, pois se houver problemas no trajeto das informações, pode trata-se de um problema muito maior do que apenas um problema de performance e pode aferir a disponibilidade da rede (ABREU e PIRES, 2004). Obtendo-se sucesso na conectividade, opções mais avançadas podem ser usadas para melhorar as aplicações e recursos utilizados.

5.3.2 Tempo de resposta

O tempo necessário para que um pacote viaje entre dois hosts na rede é denominado tempo de resposta, e durante o trajeto podem ocorrer alguns fatores que influenciam nesse tempo de resposta, como a sobrecarga de processamento, erros de sistemas, falha ao acesso e nos dispositivos da rede (ABREU e PIRES, 2004).

Normalmente o tempo de resposta é medido no instante em que ocorre o tráfego dos pacotes entre o emissor e o receptor, sendo controlado pelo gerenciamento de desempenho que mostra o tempo médio de resposta e os horários de pico, pois qualquer alteração ou aumento nesse tempo é uma indicação de que a rede está operando acima da sua capacidade de processamento (FOROUZAN, 2010).

5.3.3 Utilização da rede

A utilização da rede é baseada através dos recursos utilizados e da mensuração de performance, medido não apenas em termos de atraso, mas em probabilidades de perda de pacotes e para cobrir essa objeção os administradores utilizam modelos de desempenho que quantifica uma determinada carga de processamento, alocando a largura de banda a um custo mínimo (KUROSE, 2013).

O aspecto principal que influencia a rede segundo Abreu e Pires (2004), é o emprego de cada segmento situado na comunicação, o caminho entre dois dispositivos, essa utilização é referente a um pequeno percentual das informações transmitidas e recebidas em um determinado período de tempo, a maioria das ferramentas de performance utilizam diferentes elementos, a vazão (throughput) e a capacidade de transmissão da rede são alguns exemplos.

5.3.4 Vazão

A vazão equivale indicar a quantidade de banda disponível para as aplicações em determinados momentos, sendo a quantidade de *bits* enviando e influenciados diretamente por gargalos durante o tráfego, pois mesmo que um enlace de comunicação alcance 100 Mbps, essa velocidade não permanecerá fim a fim (ABREU e PIRES, 2004).

5.3.5 Capacidade de transmissão da rede

A capacidade de processamento de enlaces está ligada ao *throughput*, taxa de transferência, modo como os dados trafegam de um lugar ao outro. Para determinar a variação da transmissão é utilizado técnicas como *packet pair* e *packet trains*, no qual o primeiro envia um par de pacotes remotamente para um dispositivo com intervalo de tempo e o segundo é a variação de tempo do pacote percorrido até chegar ao destino (ABREU e PIRES, 2004). A

forma como cada pacote viaja de um lugar a outro determina a qualidade do tráfego e um congestionamento pode afetar a carga da rede, diminuindo assim a taxa de velocidade.

De acordo com Kurose (2013) “a capacidade de transmissão do enlace será compartilhada pacote por pacote somente entre usuários que tenham pacotes que precisam ser transmitidos pelo enlace.”

5.4 Ferramenta zabbix

Conforme Kurose (2010), para que a rede seja administrada de forma adequada, é necessário que se tenha o monitoramento constante da rede com uso de ferramentas que auxiliem o administrador para ter controle sobre ela.

Antes do seguimento do conteúdo com as características da ferramenta Zabbix, para fins de comparação de ferramentas de monitoramento, elaborou-se uma tabela, exibida abaixo, com base no artigo de Kharb (2019) e Santos et. al. (2016) onde estes comparam algumas das principais ferramentas de monitoramento de rede.

Tabela 1 - Comparação de ferramentas de monitoramento

Comparação de ferramentas utilizadas para monitoramento de redes						
Ferramenta	Licença	Métodos de armazenamento de dados	SNMP	Agentes	Plataforma	Recursos gráficos
Cacti	Sim	MySQL	Sim	Não	C++, Java	Sim
Collectl	Não	Sim	Sim	Não encontrado	Perl	Não
Nagios	Sim	Sim	Por Plugin	Suportado	C	Sim
Open NMS	Sim	Sim	Sim	Suportado	Java	Sim
Zabbix	Sim	Sim	Sim	Suportado	C, PHP	Sim

Fonte: Autores

De forma básica, a identificação dos itens da tabela, tem-se o parâmetro “licença” que se dá pela característica de poder modificar, estudar, compartilhar ou não o software. No parâmetro "método de armazenamento de dados” seria correspondente ao caso da a ferramenta conter possibilidades de armazenamento diferentes, ou simplesmente conter algum tipo de

armazenamento local. Sobre o parâmetro “SNMP” se trata basicamente se a ferramenta trabalha com a utilização deste protocolo. No parâmetro de “Agentes” refere-se a utilização de agentes para a coleta de dados, próprio da ferramenta. “Plataforma” se trata da linguagem da ferramenta, e recursos gráficos, se refere a possibilidade de criar mapas e graficos com a ferramenta.

Em detrimento às outras ferramentas de monitoramento de rede, a escolha da ferramenta Zabbix para monitoramento da rede de computadores do SESI SENAI DR - AP, se deu pelo conhecimento e familiaridade da equipe de T.I já consolidado sobre a ferramenta por já terem trabalhado com o Zabbix.

Além disso, o Zabbix é uma ferramenta *open-source* (Código aberto) para monitorar a rede de computadores, servidores e serviços, gerenciando o fluxo de atividades e disponibilizando uma boa experiência e qualidade de serviços. A ferramenta de gerenciamento foi criada pelo Alexei Vladishev e atualmente é desenvolvida pela Zabbix SIA, com escritórios abertos na Europa, EUA, Japão, Rússia e América Latina para aprimorar o desenvolvimento do software, facilitar o contato com os usuários locais e oferecer o suporte necessário (Zabbix, 2022).

A solução *open-source* usa um mecanismo de notificação flexível que permite aos usuários configurar os e-mails para receber alertas sobre alguma inconsistência nos serviços, permitindo uma reação rápida aos problemas da rede (Zabbix, 2022). Além disso, é uma ferramenta que disponibiliza relatórios e visualização de dados obtidos com excelentes características baseado nas configurações armazenadas.

Devido a gama de recursos que o Zabbix oferece, o software é disponível em diversas plataformas operacionais que entregam de forma consistente os requisitos de performance. O UNIX é sistema operacional com performance intolerante a falhas e o Zabbix é compatível em plataformas com o Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, MAC-OS, Solaris e Windows por meio de agentes na versão desktop e versões de servidor desde o XP (Zabbix, 2022).

5.4.1 Funcionamento

O *Zabbix* é uma solução desenvolvida para monitorar o funcionamento do sistema de rede. De acordo com Zabbix (2022), a ferramenta provê inúmeros recursos de gerenciamento e monitoração em um único pacote, disponibilizado em seu site com funcionalidades básicas de uma solução de controle baseado em três componentes, Banco de dados, *Zabbix Server* e

Interface *Web*. As informações de configuração do gerenciamento feito são armazenadas no banco de dados, e tanto o Servidor quanto a Interface *Web* do *Zabbix* interagem com o SGBD (Sistema de Gerenciamento de Banco de Dados).

5.4.2 Zabbix Banco de Dados

Segundo o site do Zabbix (2022), o banco de dados do Zabbix é um agrupamento de informações armazenadas em um Sistema de Gerenciamento de Banco de Dados em dois formatos, históricos e médias. O formato histórico guarda todos os valores coletados sem nenhuma sumarização, ou seja, na forma íntegra, por outro lado as médias já guardam de forma sumarizada de hora a hora, visando a geração de gráficos e outras informações com um custo menor de processamento para o banco de dados.

O uso da coleta de dados é uma atividade que visa captar conteúdos importantes sobre os serviços gerados, como verificações de disponibilidade e desempenho por exemplo, podendo ser executado pelo servidor, *proxy* ou pelos agentes, além de suportar vários protocolos de gerenciamento para monitoração e as verificações são personalizadas por meio da função de agendamento (Zabbix, 2022).

A coleta de dados dos itens no Zabbix é feita no conceito de Intervalo entre coletas. Em versões anteriores do Zabbix existia a possibilidade de ter um intervalo padrão e um intervalo flexível, entretanto não era possível informar um momento específico para a coleta de dados do item. Agora, a partir do Zabbix 3.0 tornou-se possível definir essa coleta e também o agendamento de coleta, podendo ser definido os dias e horários específicos para coletar os dados gerados (Zabbix, 2022).

5.4.3 Servidor Zabbix

De acordo com Júnior (1999, p.358) “O computador gerente é considerado como o coração do sistema de gerenciamento de rede e como tal deve-se fornecer atenção redobrada ao mesmo.”

O servidor do Zabbix é considerado toda inteligência de monitoramento, responsável por gerenciar o repositório central de configuração, estatísticas e armazenamento de dados operacionais, além de alertar os administradores quando os incidentes ocorrerem, sendo esse o componente central da solução (SILVA, 2021).

Segundo o site do Zabbix SIA (2022), o servidor gerencia o recebimento de dados, calcula o estado de cada um, envia notificações alertando o administrador sobre o funcionamento e é o componente para o qual os agentes e *proxies* enviam dados sobre a disponibilidade, performance e integridade dos sistemas monitorados. Em ambientes centralizados, os agentes enviam os dados coletados para ele informando sobre integridade, disponibilidade e a estatística de cada um. Em ambientes descentralizados o envio dos dados é feito para um componente intermediário chamado *proxy*.

Para manter o controle de cada equipamento, o Zabbix utiliza ferramentas de monitoramento capazes de oferecer excelentes relatórios com base em funcionalidades que a ferramenta dispõe. O servidor é o responsável por centralizar essas informações advindas do *host* e do grupo de *hosts*, item, gatilho, evento, *trigger*, regra de descoberta, mapas, comando remoto, notificações, *dashboard*, entre muitas outras ferramentas (Zabbix, 2022)

Em definição, o *host* é o monitoramento dos dispositivos com IP/DNS e o grupo de *hosts* é uma expressão lógica dos agrupamentos de hosts, o item é usado para receber métricas dos *hosts*, o gatilho define os limites de problemas, o evento é uma eventualidade que ocorre na rede e merece uma atenção no local, a *trigger* é uma expressão lógica usada para analisar os dados coletados pelos itens, a regra de descoberta automatiza a rede em relação aos dispositivos, os mapas são utilizados para visualizar o monitoramento, assim como o *dashboard*, já o comando remoto executa automaticamente comando nos *hosts* e as notificações servem para informar os administradores sobre os acontecimentos da rede (Zabbix, 2022).

5.4.4 Zabbix Web

Na interface *Web* do *Zabbix* é possível visualizar as informações da rede, sendo o responsável pela visualização, gerenciamento de configuração e execução dos *scripts* via interface (SILVA, 2021). De acordo com o site oficial do *Zabbix*, o *front-end*, como também é conhecido, é o recurso que o diferencia de outras soluções, pois apresenta uma GUI (*Graphical User Interface* ou Interface Gráfica do Usuário) poderosa e fácil de usar, fornecida com o pacote padrão. É uma interface que fornece acesso não intimidante para usuários iniciantes e recursos de configuração em larga escala para diversas instalações.

5.4.5 Agente Zabbix

O Agente *Zabbix* é um componente de solução implementado na máquina de destino que precisa ser monitorado para coletar informações operacionais e relatar os dados ao *Zabbix Server* para o processamento adicional e se houver ocorrência de falhas, o *Zabbix Server* informa aos administradores sobre a máquina que apresentou problemas (Zabbix, 2022).

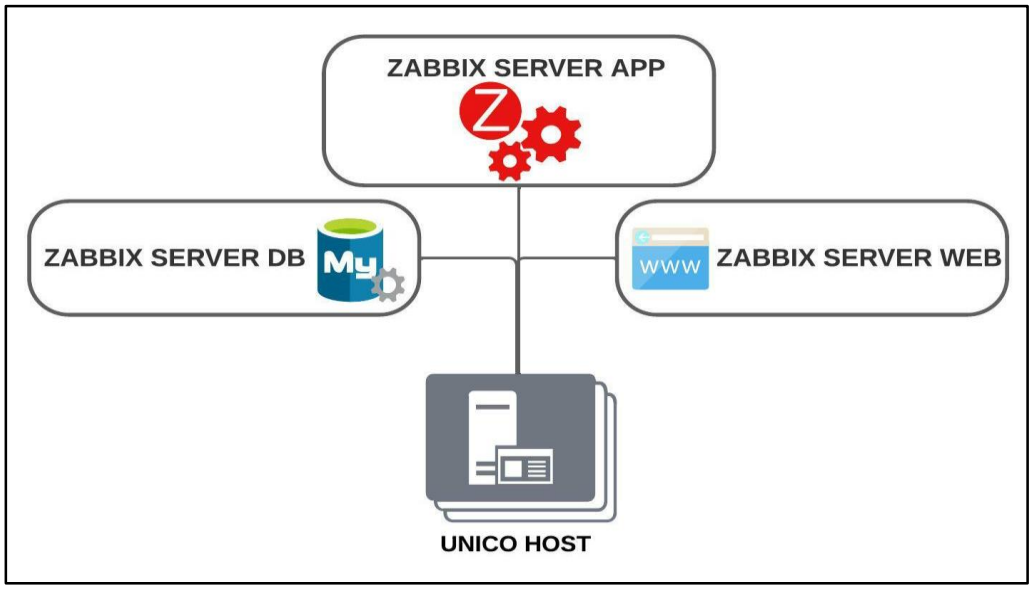
Um *Agente Zabbix* nativo, desenvolvido em linguagem C, pode ser executado em várias plataformas suportadas, incluindo *Linux*, UNIX e *Windows*, coleta dados como CPU, memória, disco e uso de interface de rede de um dispositivo. Além de ser extremamente eficiente em relação ao uso de chamadas de sistemas nativas para coleta de informações, podendo realizar verificações passivas ou ativas (Zabbix, 2022).

Em uma verificação passiva, o agente responde a uma solicitação de dados do servidor Zabbix (ou *proxy*), como um pedido sobre a carga da CPU por exemplo, e então o agente Zabbix envia de volta o resultado com a resposta para o servidor. Em relação às verificações ativas, o agente primeiro recupera uma lista de itens do servidor Zabbix para processamento e em seguida, envia periodicamente novos valores para o servidor, permitindo que o agente continue executando o perfil de monitoração mesmo quando o servidor Zabbix estiver indisponível (Zabbix, 2022).

5.4.6 Estrutura de Camadas

Essa referenciação em “camadas” faz alusão a arquitetura utilizada quando faz-se a instalação do serviço Zabbix para monitorar um ambiente de produção, há o modo *All in one* (tudo em um), exemplificado na figura 1, que ocorre quando se implementa o serviço todo em um só *host*, então, o *Zabbix server, front-end* e Banco de dados somente em uma máquina, disputando por processamento, espaço em disco e espaço na memória volátil (SILVA, 2021).

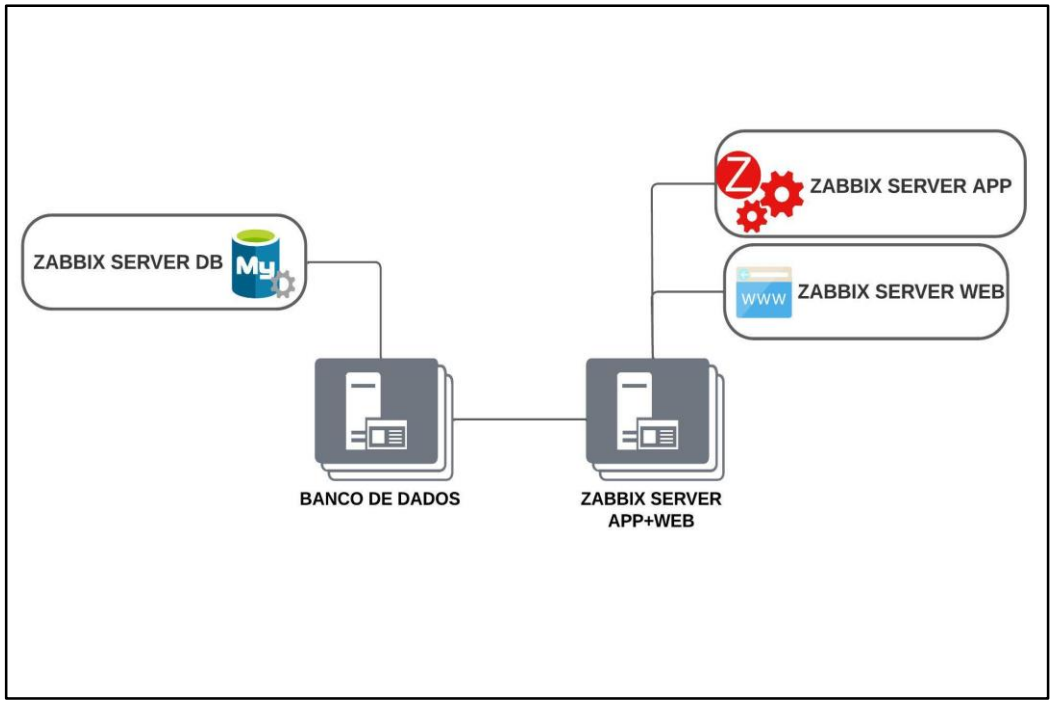
Figura 1 - Exemplo de instalação de *All in one*.



Fonte: Autores

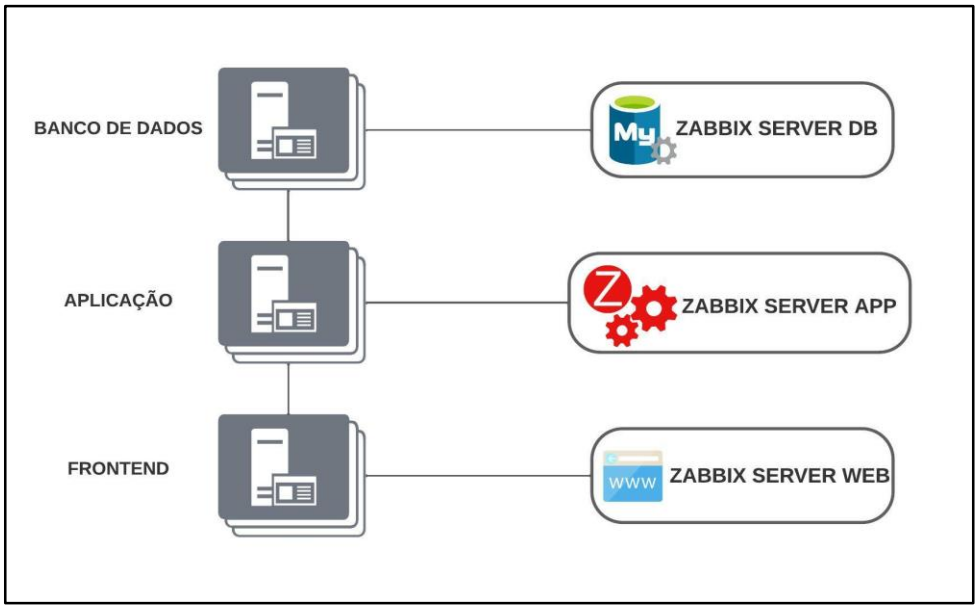
Outro modo como aborda Silva (2021) é fazer em "camadas", utilizando *hosts* diferentes, por exemplo, 2 camadas (duas máquinas diferentes) uma para o Zabbix *server* e *front-end* e a outra para o banco de dados, conforme exemplificado na figura 2, e 3 camadas (três máquinas diferentes) uma para o Zabbix *server*, outra para o *front-end* e a última para o banco de dados, conforme exemplificado na figura 3.

Figura 2 - Exemplo de instalação de 2 camadas



Fonte: Autores

Figura 3 - Exemplo de instalação de 3 camadas



Fonte: Autores

Corroborando Rodrigues (2022) recomenda-se utilizar a estrutura de instalação do Zabbix em forma de camadas quando o cenário é o próprio ambiente de produção. Dependendo do ambiente e da quantidade de objetos monitorados, o processamento e armazenamento dos serviços irão variar muito. Por isso, com a separação dos serviços em camadas (em *hosts* diferentes) tornam os *hosts* customizáveis ao serviço que estão hospedando e com isso, nenhum serviço estaria disputando por processamento, espaço em disco (leitura e escrita) ou memória RAM (*Random Access Memory*).

Tomando como base o artigo do portal Teleco (2012) Um *software* de gerenciamento é composto basicamente por elementos gerenciados, agentes, gerentes, banco de dados, protocolo para troca de informações de gerenciamento, interfaces para programas aplicativos e interfaces com o usuário.

Resumidamente, pode-se dividir o *Software* de gerenciamento em três categorias: *Software* de apresentação para o usuário (interface), *Software* para gerenciamento da rede (aplicação) e *Software* de suporte (banco de dados e a comunicação).

Tendo isso em vista, juntando os estudos citados acima, chega-se ao ponto de segmentar o *software* de gerenciamento visando a estabilidade, desempenho, segurança e escalabilidade do serviço. Dividindo-o em 3 camadas, uma camada para o *Software* de apresentação para o usuário (interface) (serviço *front-end*), outra camada para o *Software* para gerenciamento da rede (aplicação) (serviço da aplicação Zabbix - *Zabbix server*) e a última camada para o *Software* de suporte (banco de dados e a comunicação) (Banco de dados do Zabbix).

6 TRABALHOS RELACIONADOS

Neste trabalho tem-se o objetivo de implementar e exibir o exercício da ferramenta da *Zabbix* baseado em modelos que agreguem na infraestrutura de rede do SESI SENAI DR - AP e para isso foi pesquisado referências para utilizar na implementação. Ademais, nessa sessão é explorado algumas pesquisas utilizando essa ferramenta como gerenciador de equipamentos na rede para analisar aspectos úteis dessa implementação.

Nesta pesquisa [Castro, Carvalho et al. 2013] é explorado três ferramentas de monitoramento para a gestão de rede: o *Cacti*, o *Zabbix* e o *The Dud*e. Com intuito de incentivar o uso de um desses serviços em empresas e pela equipe de TI, eles demonstram soluções feitas para evitar possíveis falhas na rede com o uso da própria ferramenta que está monitorando os serviços ou equipamentos e realizam comparações entre elas. Esses programas têm a função de analisar toda infraestrutura de rede e fazer alertas por e-mail ou por SMS sobre a indisponibilidade de qualquer serviço ou dispositivo. No trabalho é apresentado estudos teóricos sobre o gerenciamento junto com as características, instalação e configuração de cada ferramenta de gerência e demonstrações práticas para diferenciar cada tipo de serviço a partir das informações coletadas. Ao final, concluiu-se que todas as ferramentas mostraram ser eficientes com o gerenciamento, bastando o administrador configurá-las de maneira adequada para o ambiente desejado.

O trabalho de [Teodoro, 2013] visa demonstrar as vantagens em ter uma rede monitorada através de uma simulação com dois cenários de rede, onde o primeiro cenário não possui nenhum tipo de monitoramento e no segundo o autor conta com um sistema NMS (*Network 13 Management System*) para coletar informações via agentes, enviar para uma estação de gerenciamento e utilizar o *Zabbix* como gerenciador de rede por possuir uma interface *web*, demonstrar as máquinas no *front-end* e armazenar as informações no banco de dados.

No artigo [Bahls, 2016] apresenta a problemática do crescimento no uso de computadores e a necessidade da implementação de ferramentas para auxiliar o profissional da rede a gerenciá-las devido a falhas ocorridas no ambiente. Para isso, foi criado um cenário com intuito de implementar uma ferramenta de gerenciamento de equipamentos utilizando o *Zabbix* para diminuir a intervenção direta do administrador, além de trabalhar com o modelo FCAPS para atingir informações mais precisas dos equipamentos. Na estrutura da rede consistiu em trabalhar com um servidor de gerenciamento no qual foi instalado o servidor *Zabbix* e um servidor *web Apache*, um servidor *DNS Bind*, um servidor DHCP e um servidor de arquivos

Samba na estrutura a ser monitorada. A versão do *Zabbix* utilizada foi a 3.0 LTS em um sistema operacional *CentOS* 7, com os passos de instalação, configuração e os dashboard presente na interface *web* do *Zabbix* que mostra o monitoramento dos equipamentos. Analisando o cenário, o uso da ferramenta mostrou-se versátil e de fácil instalação, permitindo assim reduzir o tempo de indisponibilidade dos serviços ao usuário final e monitorar visualmente toda a infraestrutura da rede, porém neste trabalho não há um detalhamento do ambiente no qual foi usado a ferramenta *Zabbix*.

Este artigo de [Braga, Colares et al. 2019] apresenta que o gerenciamento é essencial para que a rede mantenha um bom desempenho e como ambiente de estudo é apresentada a rede do Instituto Federal Catarinense por utilizar a ferramenta Zabbix. Com isso, o objetivo do trabalho foi aplicar um questionário para os usuários da rede do instituto e realizar uma comparação com os gráficos apresentados pelo Zabbix para analisar a percepção dos usuários em relação ao desempenho da rede cabeada e o *Wi-fi*. Os procedimentos metodológicos adotados foram o google forms para fazer o questionário referente a rede e a análise dos gráficos da ferramenta de gerenciamento. Por fim, com os resultados obtidos, concluiu-se que os gráficos gerados pelo Zabbix coincidem com o questionário feito para os usuários, apresentando os níveis de potência da rede e o auxílio dessa ferramenta para a análise em questão.

7 METODOLOGIA

Para a coleta de dados, a pesquisa foi elaborada com base em dados secundários existentes sobre o assunto de gerenciamento de redes e o monitoramento com a ferramenta *Zabbix*, assim cita Gil (2002) pesquisas que tomam como embasamento livros, artigos e até revistas sobre o determinado assunto referido no estudo, essas pesquisas podem ser classificadas como bibliográficas. Outro ponto é que a mesma ainda conta com a vantagem de fornecer mais conteúdo sobre o objeto do estudo de forma ampla do que o modo de pesquisa que é feito diretamente pelo pesquisador (GIL, 2008).

Com o intuito de aprofundar o conhecimento sobre o *software* de gestão *Zabbix* para o gerenciamento e monitoramento dos ativos no ambiente de rede, através de uma implementação em uma infraestrutura de TI, caracteriza-se essa pesquisa como de caráter aplicada que de acordo com Gerhardt e Silveira (2009, p.35) “este tipo de pesquisa tem como objetivo gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos”.

Em relação ao procedimento para conhecer o funcionamento do *software Zabbix*, define este trabalho como pesquisa experimental, conforme explica Raupp (2006), nesse tipo de procedimento o pesquisador cria um cenário para fazer o experimento, no qual controla as variáveis e analisa o efeito e causa com base nos resultados. Para atingir as finalidades estabelecidas acerca do tema, elaborou-se a instalação do *Zabbix* e a experimentação prática nos equipamentos a serem monitorados.

Em relação ao objetivo da pesquisa, caracteriza-se a mesma como exploratória devido ao percurso adotado, assim como cita Cervo, Bervian e Silva (2007), a pesquisa exploratória é recomendada quando há pouco conhecimento sobre o problema a ser estudado. Tomando como base Gil (2002) uma vez que a pesquisa se denomina exploratória, ela consiste em ter uma maior proximidade com o universo do objeto de estudo pesquisado. Precisa-se aprofundar o conhecimento do tema retratado no trabalho a fim de documentá-lo através de experimentos em simulações para servir de base para aplicações no cotidiano.

Para fazer a análise dos dados coletados, este estudo caracteriza-se como uma pesquisa qualitativa, em que segundo Pereira *et al.* (2018) os métodos qualitativos são aqueles nos quais é importante a interpretação feita por parte do pesquisador em relação ao estudo, abordando uma visão clara sobre os resultados obtidos acerca do fenômeno em que está sendo pautado. Assim, aqui visa analisar o tempo de resposta entre o alerta feito pela ferramenta Zabbix para

administrador, constatando alguma inatividade dos equipamentos, serviços e sistemas, além de verificar a performance da rede através da interface *Web*.

Partindo da teoria, o método científico utilizado para chegar a conclusão sobre o funcionamento da ferramenta *Zabbix* em relação a gerência de redes foi o método dedutivo que de acordo com Pereira et al. (2018) se o conhecimento é insuficiente para explicar uma dedução, surge um problema e em seguida hipóteses para formulá-los, logo deduzem-se consequências a serem testadas ou falseadas.

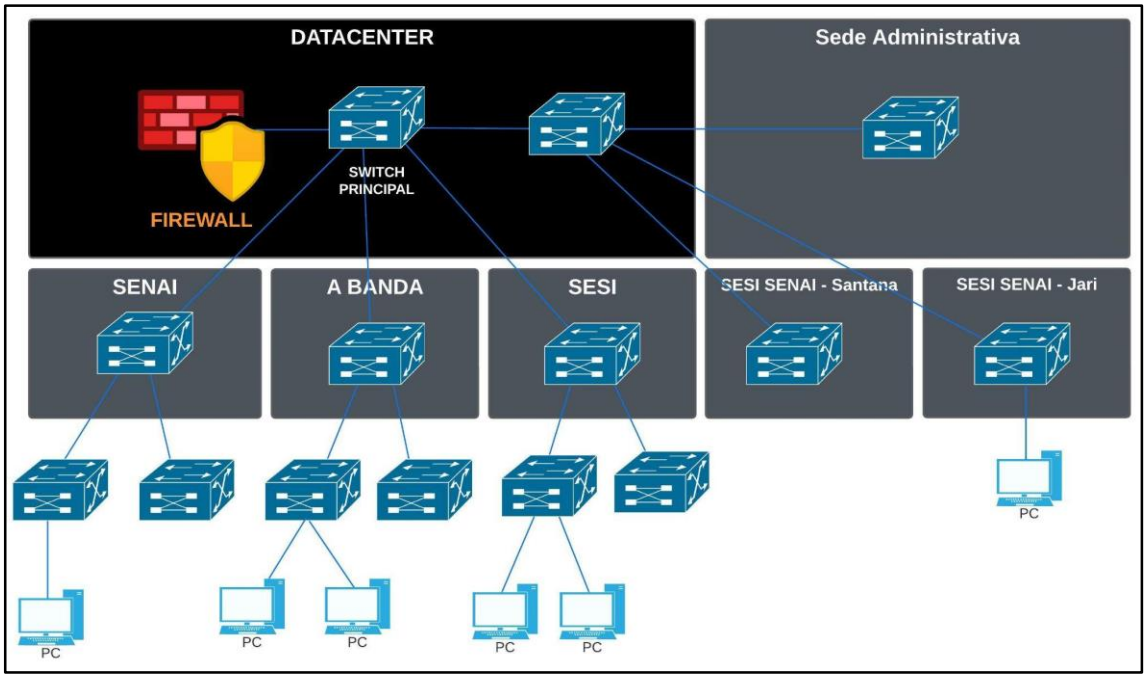
8 ESTUDO DE CASO

Nesta seção, para maior compreensão do cenário utilizado, será apresentado à rede de computadores presente no SESI SENAI DR - AP e suas demais unidades. Por questão de privacidade, segurança e integridade da infraestrutura de rede, o departamento de T.I e autores deste artigo optaram por não divulgar os endereços IP's dos equipamentos, contudo é claramente possível entender os diagramas de rede. Sendo assim, ao decorrer desta seção os endereços IP’s serão retirados ou tapados dos mapas e *Dashboards*.

Partindo para a caracterização topológica da infraestrutura utilizada no SESI SENAI DR - AP, é identificado uma topologia baseada em estrela estendida que se trata de uma variação da topologia estrela. O funcionamento da topologia estrela se dá quando tem somente um nó central conectado a todos os outros computadores. Já na topologia de estrela estendida, os computadores se conectam a nós que, por sua vez, estão conectados ao nó central, então tecnicamente se trata de topologia estrela em longa escala.

Na figura 4, há uma ilustração que serve para demonstrar a topologia utilizada no SESI SENAI DR - AP, mostrando as conexões desde o *Data Center*, localizado na Sede Administrativa do SESI SENAI DR - AP, até as outras unidades: SESI, SENAI, A BANDA, SENAI Santana e SENAI Laranjal do Jarí.

Figura 4 - Mapa de Topologia de rede SESI SENAI DR - AP



Fonte: Autores.

Como foi possível visualizar na figura acima os dispositivos finais estão ligados a um nó central que por sua vez está ligado a outro nó central, assim caracterizando uma topologia de estrela estendida. Essa imagem é referente a uma exemplificação das conexões “centrais” da rede do SESI SENAI DR - AP, por tanto se trata somente das interligações das unidades ao *Data Cente*r na Sede Administrativa do SESI SENAI, foi feita a criação dessa imagem para uma melhor exemplificação da topologia, porém, mais adiante nesse estudo de caso, será mostrado a real dimensão dos equipamentos monitorados da rede.

Sobre as unidades da empresa SESI SENAI DR - AP é importante ressaltar que tanto alguns sistemas e serviços quanto a infraestrutura de rede são comuns a todas as unidades. Portanto, basicamente, o SESI e o SENAI compartilham a mesma infraestrutura de rede, sistemas e serviços provindos do *Data Center* localizado na Sede Administrativa do SESI SENAI DR - AP.

Em cada unidade de serviço do SESI e SENAI no estado do Amapá há um CPD (Centro de Processamento de Dados) onde ficam os equipamentos topo de rack, responsáveis pela interligação da unidade com o *Data Center* estabelecendo conexão com os serviços e sistemas fornecidos pelo departamento de T.I da empresa.

Essa interligação é feita por enlaces de dados que, em alguns casos, são enlaces terceirizados pela empresa de internet contratada, para fins de compreensão a respeito dessa tomada de decisão sobre a terceirização de enlaces, faz-se necessário documentar a localização de cada unidade que está fazendo parte da rede de computadores do SESI SENAI DR - AP. Portanto, segue abaixo as localizações das unidades no estado do amapá:

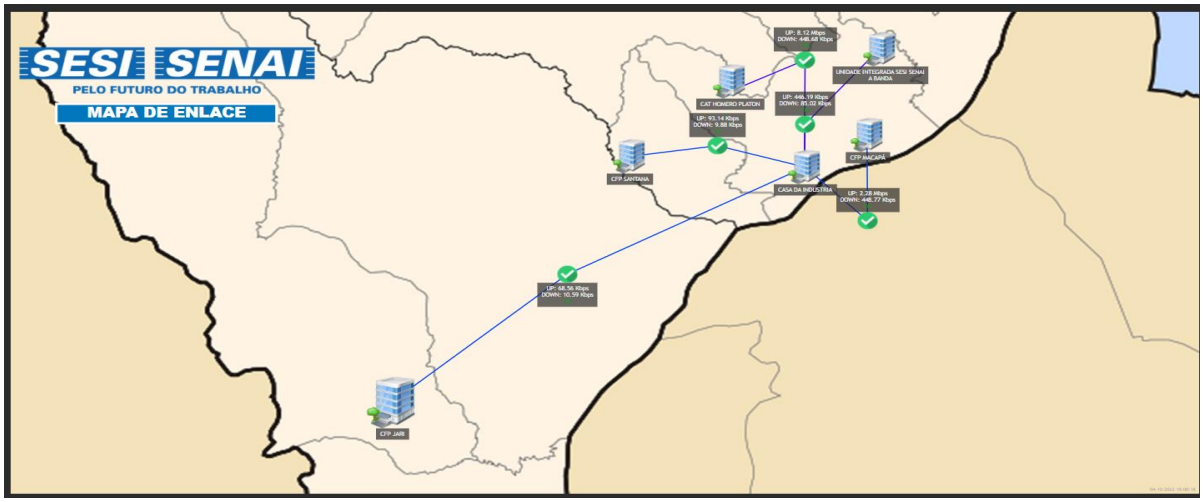
- Sede Administrativa do SESI SENAI DR - AP: Localizada na Av. Padre Júlio Maria Lombaerd, 2000 - Santa Rita, Macapá - AP, 68902-892;
- SENAI CFP Macapá - AP: Localizado na Av. Padre Júlio Maria Lombaerd, 2000 - Santa Rita, Macapá - AP, 68901-283;
- SESI CFP Macapá - AP: Localizado na Rua. Leopoldo Machado, 2749 - Central, Macapá - AP, 68901-130;
- SESI/SENAI CFP Santana - AP: Localizado na Rua. B Três, 505 - Vila Amazonas, Santana - AP, 68925-000;
- SENAI/DR Laranjal do Jari - AP: Localizado em Monte Dourado, Almeirim - PA, 68230-000.
- Unidade Integrada SESI/SENAI (A Banda) Macapá - AP: Av. Ernestino Borges, 257 - Santa Rita, Macapá - AP, 68901-077.

Em unidades mais próximas da Sede Administrativa o enlace da unidade é feito por Fibra Óptica própria da empresa, então, esse caso se aplica nas unidades: SENAI CFP Macapá, SESI CFP Macapá e Unidade integrada SSI - a BANDA.

Nas situações em unidades distantes, como o SESI SENAI da unidade de Santana e o SENAI da unidade de Laranjal do Jari, por serem unidades bem distantes do *Data Center*, optou-se por terceirizar o enlace pela empresa de internet contratada, que no caso, se trata da Mob Telecom. Além da distância, outro fator foi levado em consideração, o possível rompimento da fibra e empecilhos que o rompimento trás, causando indisponibilidade de serviço em unidades distantes, prejudicando o funcionamento da mesma. Com a terceirização a empresa de internet seria responsável por esse enlace estar em funcionamento, então toda a questão que envolve o reparo da fibra seria de atribuição da empresa de internet.

Abaixo, na Figura 5, há um mapa já criado no *Zabbix* da contextualização do cenário de enlaces terceirizados e próprios comentados nos textos logo acima:

Figura 5 - Mapa de Enlaces do SESI SENAI DR - AP



Fonte: Autores

Adentrando mais na rede de computadores do SESI SENAI, identifica-se os dispositivos localizados nos CPDs de cada unidade e um pouco mais além, chegando nos dispositivos de entrega final da infraestrutura de rede. Trata-se dos *Switches*, tanto os centrais que normalmente são chamados de *Switch Core* por interligarem as unidades ao *Data Center* quanto os da ponta da rede chamados de *Switch* de acesso ou borda por serem a ponta de acesso ao usuário na rede, normalmente localizado nos setores/departamentos da empresa.

Esses equipamentos são foco de monitoramento deste estudo de caso, além deles serem compatíveis e possíveis de monitoramento junto a ferramenta *Zabbix*, eles realizam um trabalho

importante na rede por serem os equipamentos a estabelecer comunicação com o *Data Center* e assim levarem os serviços, sistemas e conexão à internet aos funcionários.

Em sua maioria, esses equipamentos são gerenciáveis da marca *Dell* de modelo x1052 padrão empresarial com interface *web* de gerenciamento, por exceção em alguns casos, onde é utilizado o modelo x4012 *Core* de fibra para interligação de unidades e em outros casos que é utilizado outros *Switches* de marcas e modelos variados. No entanto, para evitar quaisquer problemas de incompatibilidade de sistemas e comunicação entre *Switches*, a empresa busca manter a padronização dos equipamentos, principalmente nos equipamentos *Core* de topo de rack.

Abaixo, na tabela 2, contém a totalidade de *Switches* com seus respectivos modelos utilizados na rede do SESI SENAI DR - AP.

Tabela 2 - Lista de *Switches* utilizados no SESI SENAI DR - AP.

Ficha técnica dos *Switches* monitorados				
Marca	Modelo	Portas	Velocidade	Quantidade
Dell	x1052 Gerenciável	48 4 SFP+	10/100/1000Mbps 10 Gbit	22
Dell	x4012 Gerenciável	12 SFP+	10 Gbit	2
Dlink	DES-1210-52 Gerenciável	48 2 2 SFP	10/100Mbps 10/100/1000BASE-T 10/100/1000BASE-T	1
Intelbras	SG 2404 MR	24 4 SFP	10/10/1000 Mbps 1000 Mbps	3
HP	V1910-24G	24 4 SFP	10/100/1000Mbps 1000 Mbps	1

Fonte: Dados de pesquisa (2022)

Outro equipamento foco de monitoramento são os DVR, o serviço de monitoramento de patrimônio e segurança dentro da instituição é essencial para qualquer empresa, e no SESI

SENAI não seria diferente. Nas unidades do SESI e SENAI há o serviço de câmeras de segurança gerenciados pelo departamento de T.I e utilizados pela equipe de segurança, em cada unidade tem diversas câmeras espalhadas para manter a segurança dos colaboradores, alunos e visitantes, além da segurança patrimonial.

Existe a necessidade de monitorar o funcionamento dos DVR para ter ciência se o equipamento está servindo ao seu propósito, fornecendo monitoramento pelas câmeras no local, assim estabelecendo ferramentas para a equipe de segurança e administração de cada unidade.

O sistema de câmeras de segurança é proporcionado pelos DVR de totalidade da marca Intelbras, porém em modelos diferentes como demonstrado na tabela 3 abaixo:

Tabela 3 - Lista de DVR utilizados no SESI SENAI DR - AP.

Ficha técnica dos DVR			
Marca	Modelo	Portas	Qntd
Intelbras	MHDX 1108	16	1
Intelbras	MHDX 1104	16	1
Intelbras	MHDX 3016	16	3
Intelbras	HDCVI 1016	16	1

Fonte: Dados de pesquisa (2022)

Finalizando o estudo da rede, outro alvo de monitoramento são as máquinas virtuais (VM), hospedadas tanto remotamente, em hospedagens contratadas pelo departamento de T.I do SESI SENAI DR - AP, quanto localmente no *storage* do *Data Center*.

Nessas máquinas virtuais contém sistemas e servidores utilizados no domínio do SESI SENAI DR - AP, não aprofundando tanto nas descrições dessas máquinas por questões de integridade da rede, optou-se por somente informar que essas máquinas são de extrema importância para o funcionamento do SESI SENAI DR - AP. Portanto, observa-se prioridades de monitoramento perante o serviço do *Zabbix*.

É possível monitorar máquinas virtuais com Agentes *Zabbix*, que são instalados, dependendo do sistema operacional atuante na máquina em questão, através de linhas de

comando (para máquinas *Linux*) e através de instalação por meio de *download* e execução com algumas configurações (para máquinas *Windows*).

8.1 Implementação do zabbix na rede do SESI SENAI DR - AP

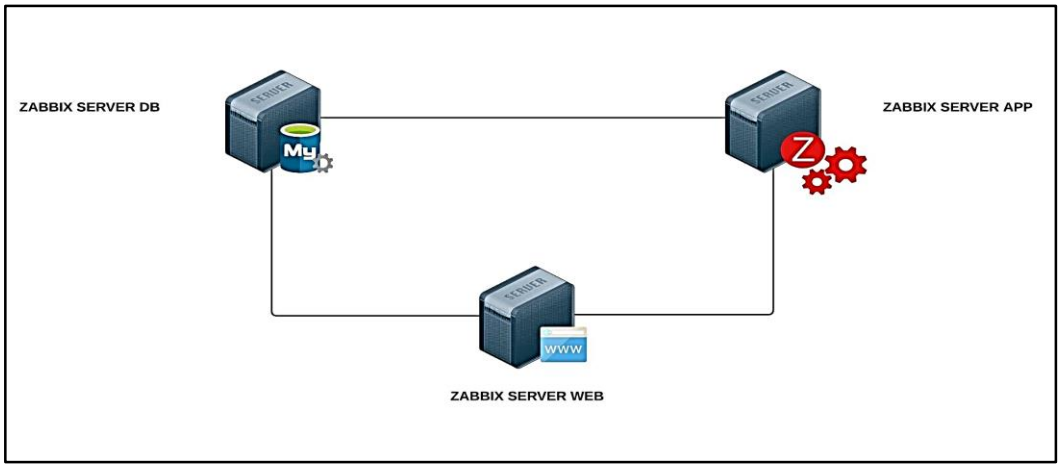
Sobre o passo a passo das instalações dos serviços que completam a solução *Zabbix* (banco de dados, *front-end*, aplicação), por questões de organização e preocupação em poluir a visualização e compreensão dos leitores, estará em forma de anexo deste estudo de caso. No entanto, a seguir, os processos da instalação estarão em uma forma de um resumo superficial do passo a passo.

8.1.1 Processo de Instalação do Serviço Zabbix

Foi utilizada a solução *VMware vSphere*, já implementada na rede do SESI SENAI, que permite criar *hosts* virtuais para a implementação de serviços ou para utilização comum de *host*, para a virtualização dos *hosts* responsáveis pelo serviço *Zabbix*. Nessa solução foi feita a criação de 3 *hosts* virtuais para a implementação do serviço em forma de 3 camadas.

Com a implementação da estrutura de camadas, foi feita a personalização dos 3 *hosts* para compor cada tipo de serviço. Abaixo segue a figura 6 demonstrando um exemplo da arquitetura do modo de 3 camadas, ficando assim:

Figura 6 - Diagrama da arquitetura de 3 camadas



Fonte: Autores

Para a camada do Banco de Dados: Como um servidor de Banco de Dados necessita de muito espaço para armazenamento dos dados coletados, foi criado um *host* no *VMware* com

bastante espaço em disco suprir essa necessidade deixando-o com 200GB de espaço. Porém, como não necessita de tanta memória e processamento para o funcionamento do banco de dados, não será extremamente necessário ter uma grande quantidade destes itens alocados na máquina. Então a mesma ficou com 4GB de memória *RAM* e 2 núcleos de processadores.

Para a camada do Servidor de Aplicação do *Zabbix*: Foi criado um *host* com especificações suficientes para suporta o processamento e alocação de vários processos de coletas na memória *RAM*, então foi adicionado ao *host* 4 núcleos de processadores e 8GB de memória *RAM*, para o armazenamento foi alocado somente 30GB de espaço em disco pois para a aplicação do serviço não necessita de tanto espaço como o Banco de Dados.

Para a camada do *Front-end* (*NGINX*): Foi criado um *host* parecido com o *host* de aplicação, porém com somente 4GB de memória *RAM*. O servidor de *Front-end* é composto somente pela aplicação do servidor *web Nginx* que foi utilizado para hospedar o serviço *web* do *Zabbix*, então, não há necessidade de alta quantidade de memória *RAM* e espaço em disco.

A conexão dessas camadas é feita através de arquivos de configuração em cada serviço, normalmente, em uma instalação *All In One* (tudo em um), não é necessário mudar as linhas de endereços nesses arquivos, pois comumente os dados em relação a conexão de outros serviços é por padrão *localhost*. Entretanto, já que é uma instalação em camadas, é necessário fazer essa alteração para que os serviços se comuniquem.

8.1.2 Processo de exportação

Na rede do SESI SENAI DR - AP havia um antigo servidor *Zabbix* 4.0.7 inativo após incidentes ocorridos na rede da empresa, porém o seu banco de dados ainda estava intacto e bastante desatualizado perante os dados dos *hosts* monitorados e versão de aplicação. Para uma reutilização de dados buscando uma forma de poupar tempo e esforço na criação e configuração de alguns mecanismos de coletas de dados do servidor *Zabbix*, foi exportado o banco de dados antigo com alguns dados importantes: *hosts*, *templates* dos *switches Dell series* 1000x e 2000x, mecanismo de alertas, históricos de incidentes e alguns mapas criados.

Mesmo com esses dados desatualizados, a melhor forma de poupar tempo e esforço foi exportar os dados em vez de criá-los um por um novamente. Esse processo, por exemplo, é bastante relevante na questão dos *hosts* antigos que ainda poderiam ser reutilizados, pois na sua maioria seriam somente alterações de endereços IP (*internet protocol*) para voltarem a ser monitorados.

Começando o processo de exportação para o servidor de banco de dados novo, tudo ocorreu de forma positiva, não houve problemas ou falhas nesse quesito. Foi utilizado como base para instrução de exportação e importação do banco de dados, a documentação oficial do *Zabbix* [3], a documentação oficial do banco de dados *Mysql* [4], e o fórum oficial do *Zabbix* [5].

A reutilização dos *templates* contribuiu na criação dos itens, *trigger*, descoberta de rede e inventário dos equipamentos de rede *Dell*, que compõem a maioria dos *switches* da rede do SESI SENAI DR - AP. Conforme as figuras 7 e 8, visualiza-se o *template* x1000 sendo utilizado nos *hosts* equivalentes aos *switches Dell* x1052, e nas figuras 9 e 10, o *switch* correspondente ao template x2000:

Figura 7 - Utilização do *template* x1000 nos *Switches*.

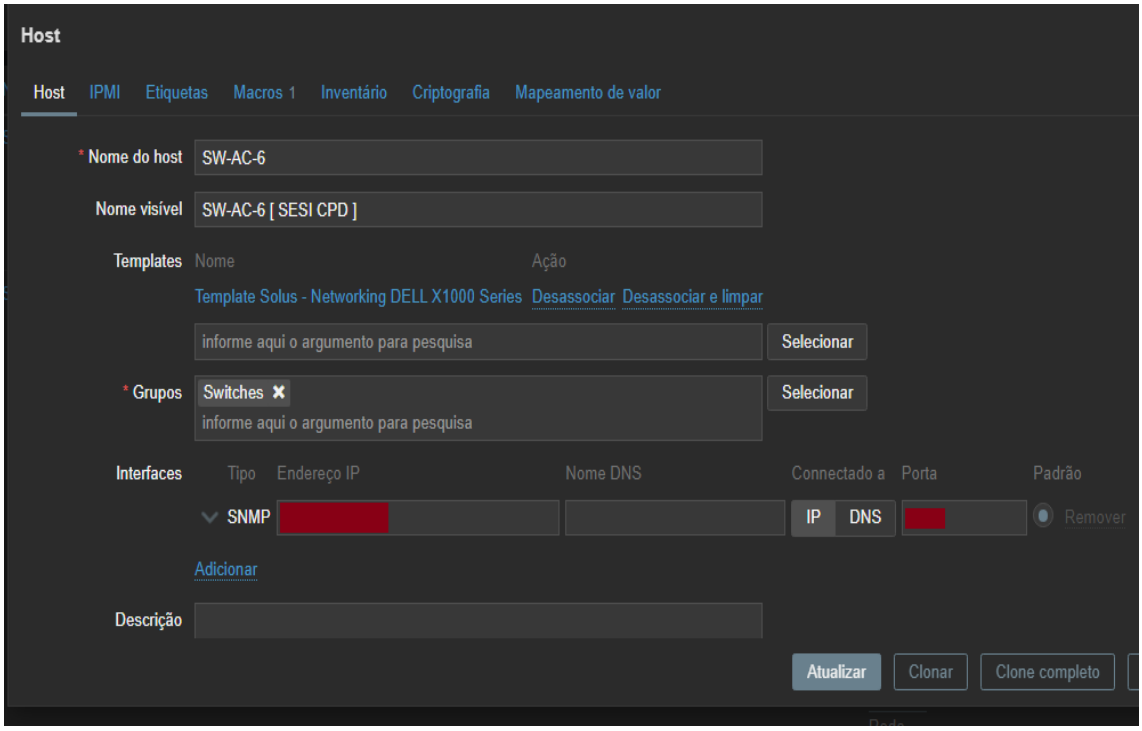
Fonte: Autores

[3] SIA, Z. Zabbix Documentation. Disponível em: <https://www.Zabbix.com/documentation/6.0/pt/manual>. Acesso em 11 de set. 2022.

[4] ORACLE, MYSQL. Documentation. Disponível em: <https://dev.mysql.com/doc/refman/8.0/en/rebuilding-tables.html>. Acesso em 8 de set. 2022.

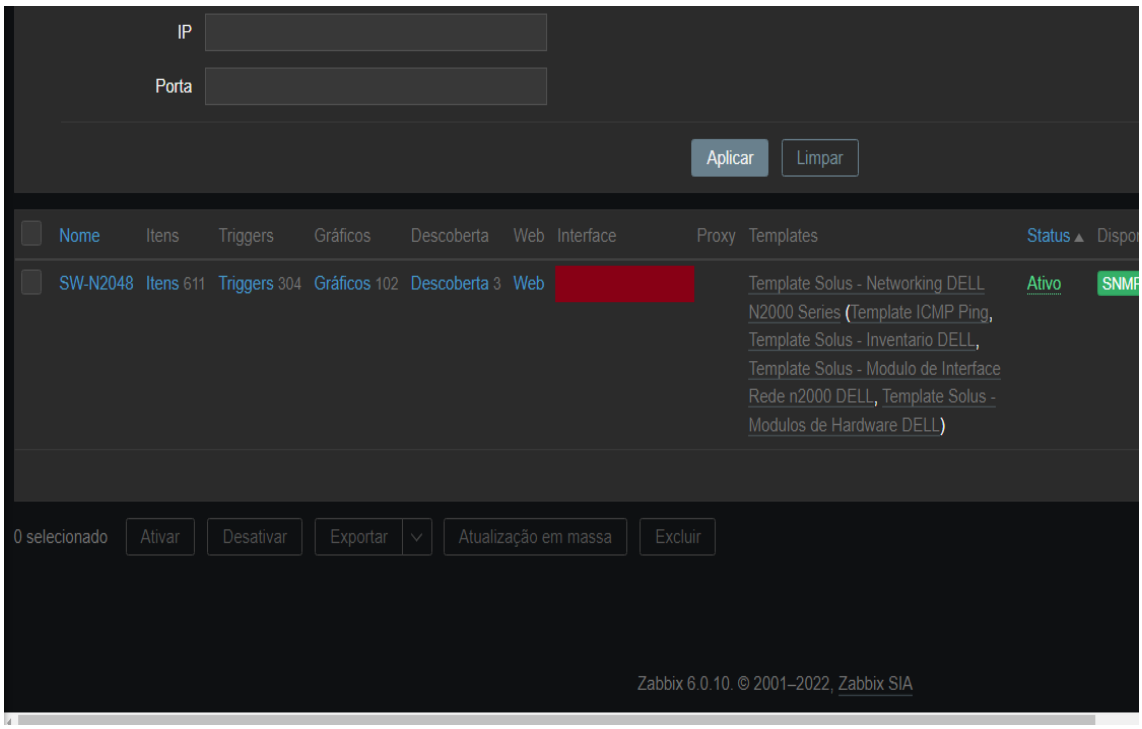
[5] SIA, Z. Zabbix Documentation. Disponível em: <https://www.Zabbix.com/forum/em-portugues-y-en-espanol/447535-exportar-importar-banco-de-dados-em-uma-nova-instala%C3%A7%C3%A3o>. Acesso em 7 set. 2022.

Figura 8 - Exemplo de *Switch* utilizando o *template* x1000.



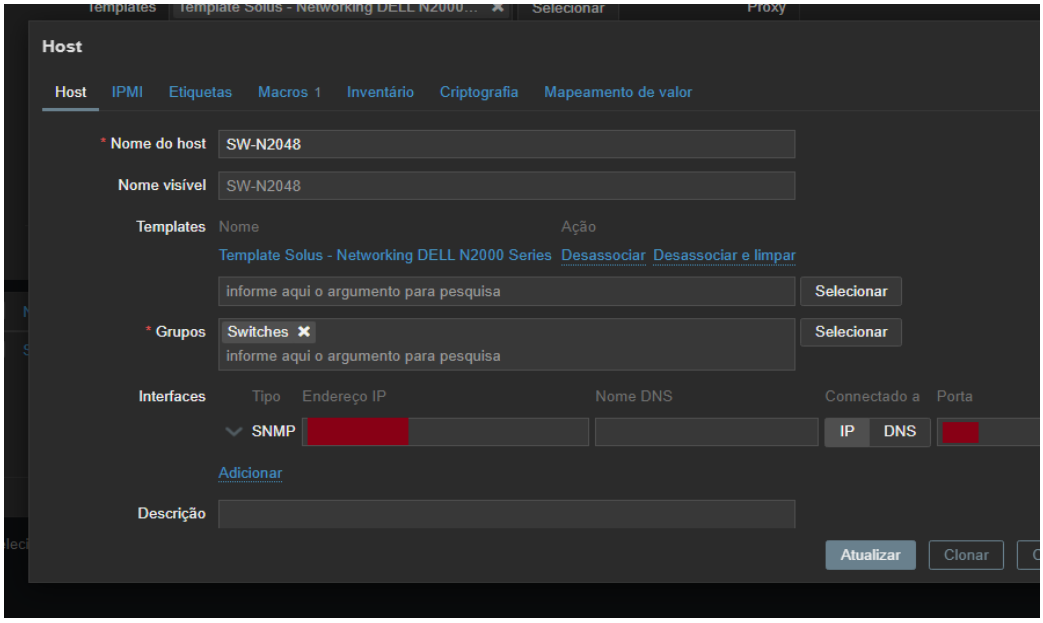
Fonte: Autores

Figura 9 - Utilização do *template* x2000 no *Switch*.



Fonte: Autores.

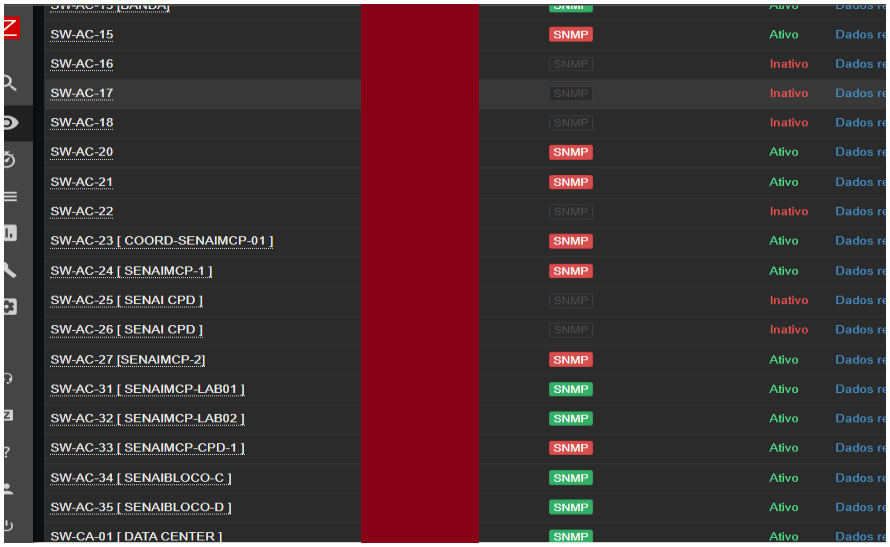
Figura 10 - Exemplo de *Switch* utilizando o *template* x2000**.**



Fonte: Autores.

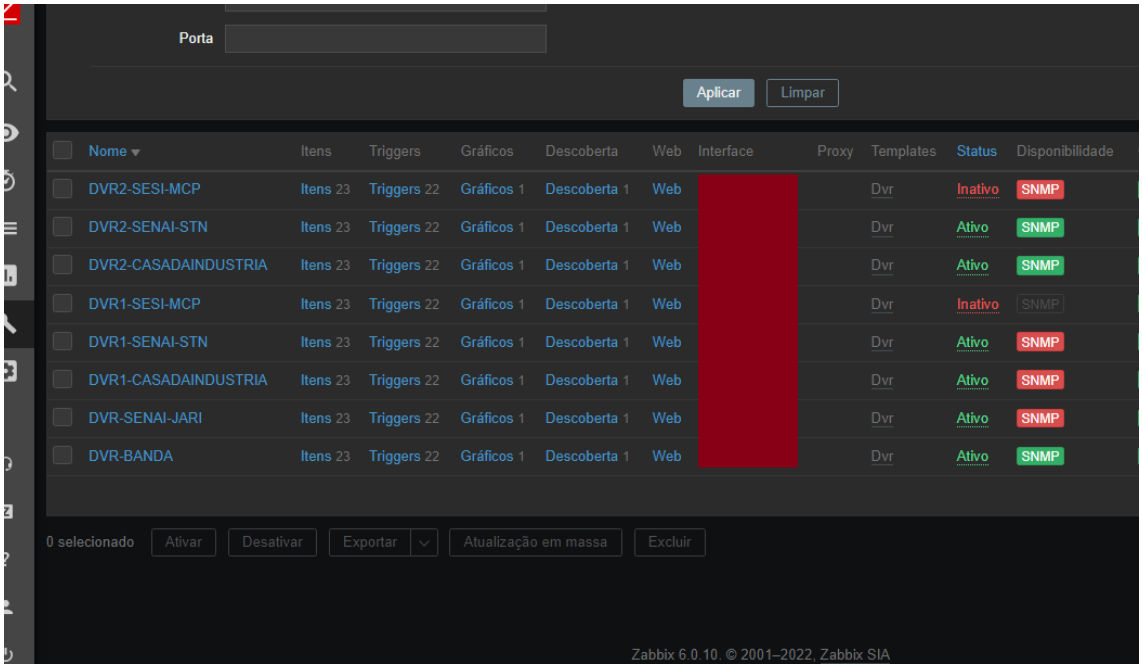
Sobre a reutilização dos *hosts* exportados, as configurações dos antigos *hosts* que correspondiam a maioria dos equipamentos ativos na rede de computadores do SESI SENAI DR - AP foram restauradas, porém, alguns com os IP's e nomenclatura desatualizados, onde foi necessário testar e verificar *host* por *host* se estavam se comunicando com o servidor *Zabbix*. Nas figuras 11, 12 e 13, são mostrados alguns *hosts* ainda desatualizados ou inativos/desativados que precisam passar pelo processo de atualização.

Figura 11 - Lista de *hosts* switch antes da atualização.



Fonte: Autores.

Figura 12 - Lista de *hosts* DVR antes da atualização.



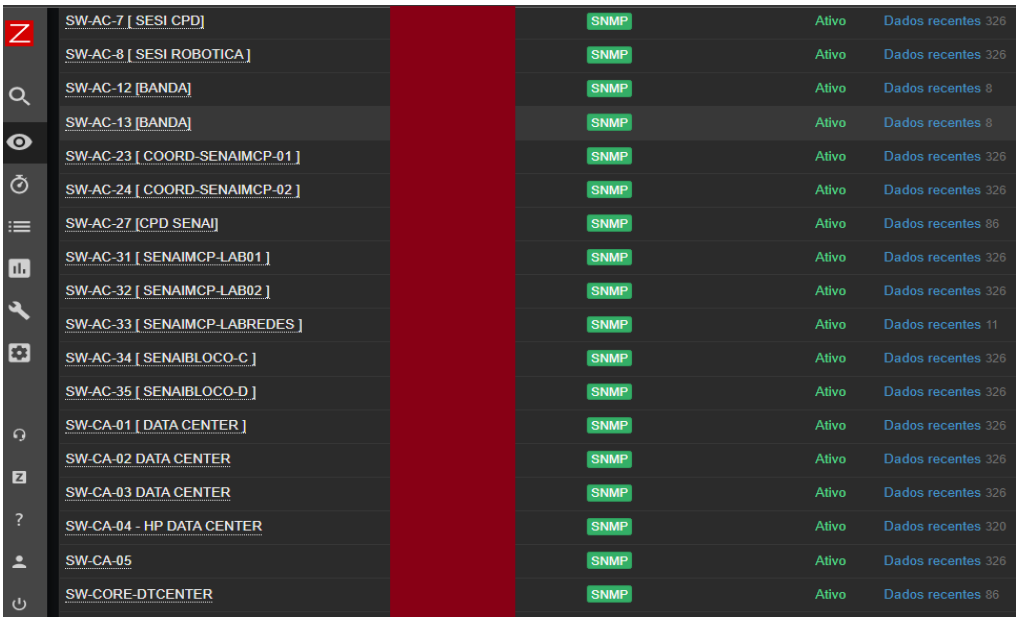
Fonte: Autores.

Figura 13 - Lista de *hosts* VM antes da atualização.

Fonte: Autores.

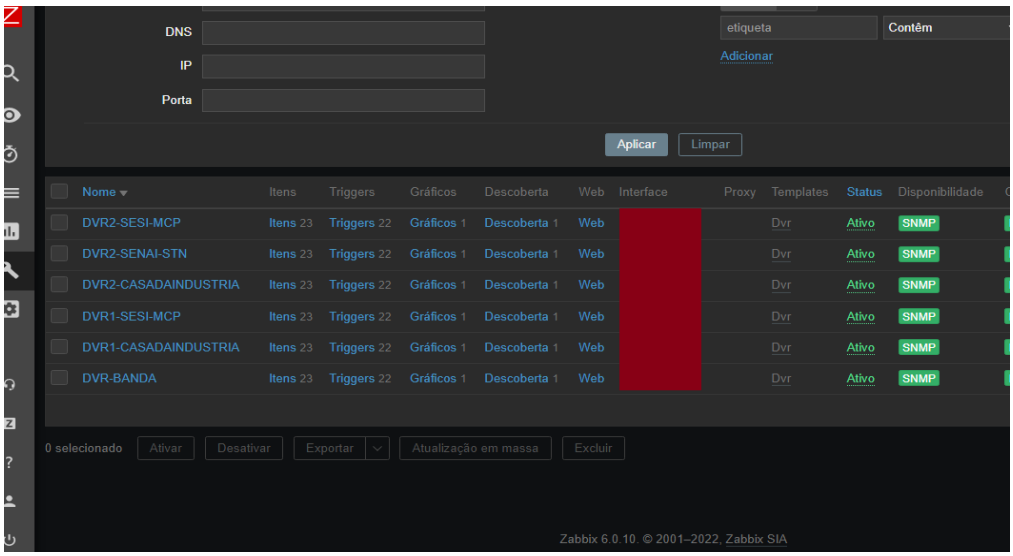
Esse processo de atualização consiste em verificar se o endereço do equipamento ainda é utilizado, verificar se há conexão com o servidor *Zabbix*, excluir os *hosts* que não estão se comunicando porque foram alterados ou desativados e inserir novos *hosts* de equipamentos novos na rede. Logo depois nas figuras 14, 15 e 16 é possível visualizar o cenário após a operação de atualização, onde é mostrado a presença de comunicação e operabilidade dos *hosts* junto ao servidor *Zabbix*.

Figura 14 - Cenário de pós atualização dos *hosts* switches.



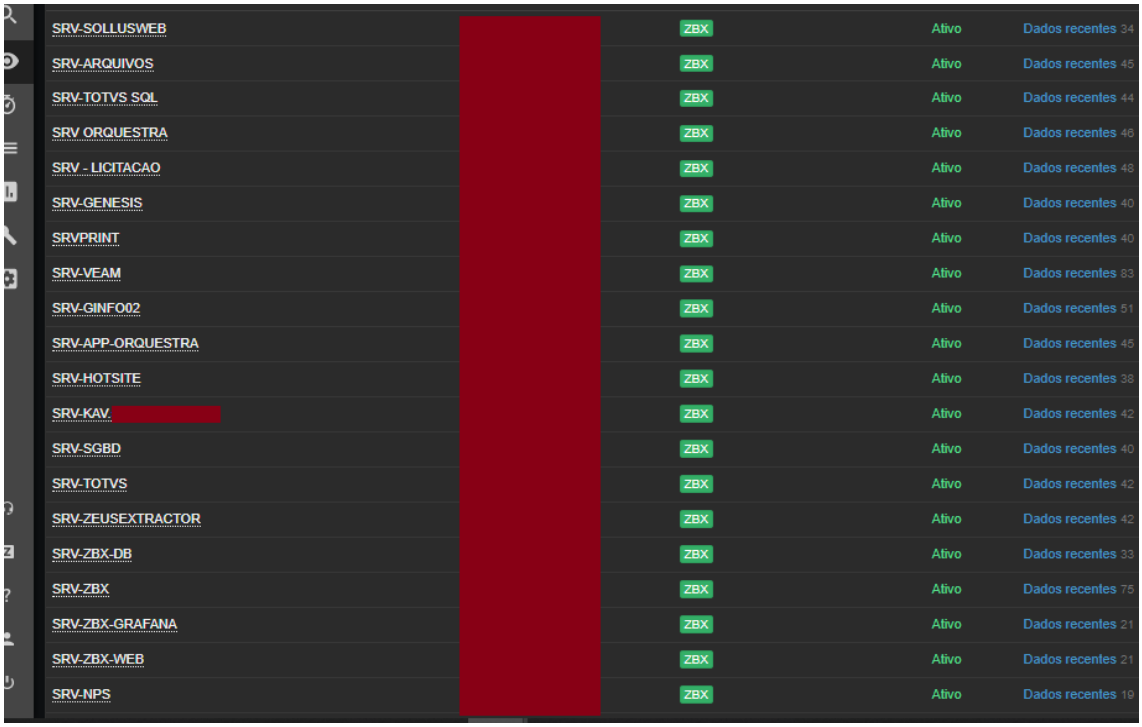
Fonte: Autores.

Figura 15 - Cenário de pós atualização dos *hosts* DVR.



Fonte: Autores.

Figura 16 - Cenário de pós atualização dos *hosts* VM.



Fonte: Autores.

8.1.3 Ferramentas utilizadas

Dentro do modelo de gestão FCAPS, que visa analisar as cinco áreas funcionais do gerenciamento de redes (falhas, configuração, contabilização, desempenho e segurança), para este estudo, foca-se no item de gerenciamento de falhas por envolver o contínuo acompanhamento dos equipamentos. Dessa maneira é possível identificar o desempenho desses dispositivos a fim de tomar medidas corretivas de forma eficaz quando necessário para que não haja indisponibilidade no sistema.

Como entende-se nos pensamentos de FCAPS sobre o gerenciamento de falhas, para esse estudo de caso, faz-se a utilização das principais ferramentas que a solução Zabbix pode oferecer para a rede do SESI SENAI DR - AP em relação ao monitoramento de falhas nos equipamentos monitorados, sendo elas:

- **Ferramenta de *hosts*:** Para utilização das outras ferramentas e formas de monitoramento é necessário a vinculação, do equipamento foco de monitoramento, a um host criado, para ele, no *Zabbix*.

- **Ferramenta de *templates*:** O *template* de um *host*, em poucas palavras, é a forma de coleta de dados que aquele *host* usa. O *Zabbix* usa esse *template* como instruções para coleta de dados daquele equipamento específico que aquele *host* está vinculado.
- **Ferramenta de *Trigger*:** Essa ferramenta do *Zabbix* é diretamente ligada ao *template* de um *host*, assim que um dado é coletado as *triggers* analisam esse dado e verificam nos seus itens se eles estão dentro do padrão estabelecido para aquele dado, se estiver ok, o status assumido na *trigger* é de operante e se estiver diferente, a *trigger* sai do operante e alarma identificando o erro, alerta ou informação.
- **Ferramenta de notificação/alarme**: Juntamente a *trigger*, existe a notificação/alarme que é operada através das análises que a *trigger* faz das coletas de dados. Essa notificação pode ser personalizada na forma de entrega ao usuário operador do *Zabbix*, nessa ferramenta é possível configurá-la para notificar, além de notificar nas telas do *Zabbix*, notificar através do *Email*, *WhatsApp*, *Telegram*, SMS e entre outros.
- **Forma de comunicação por SNMP ou por Agente *Zabbix*:** Por serem os principais meios de comunicação dos *hosts* com o *Zabbix*, nos equipamentos foco de monitoramento da rede.
- **Forma de monitoramento por Mapas, gráficos e *Dashboard*: Após** a criação e configuração dos *hosts* com alocação de *templates* e configuração de comunicação, esses *hosts* podem ser monitorados através de mapas, gráficos e *dashboards*. Basicamente são formas de visualização dos status dos equipamentos, ao longo desse estudo de caso, será demonstrado a utilização dessa ferramenta.

8.1.4 Resposta aos objetivos

Começando a etapa de apresentação dos *Dashboards* e Mapas criados em resposta aos objetivos idealizados no início deste estudo de caso, é importante reiterar que optou-se por retirar ou tapar os endereços IP’s dos equipamentos por questões de segurança e privacidade e integridade da infraestrutura de rede do SESI SENAI DR - AP.

Na figura 17 é possível visualizar a área de *Dashboard* do serviço *Zabbix*, onde é possível montá-lo de diversas formas, mostrando na forma de *slides*, em quadros (exemplo usado abaixo) e dados únicos. Nesse *Dashboard* foi escolhido os dados de conexão com a internet, mapa de geral de *switches*, informações do servidor *Zabbix* (onde mostra se o mesmo está em funcionamento, ou apresenta erros), hora e incidentes por severidades.

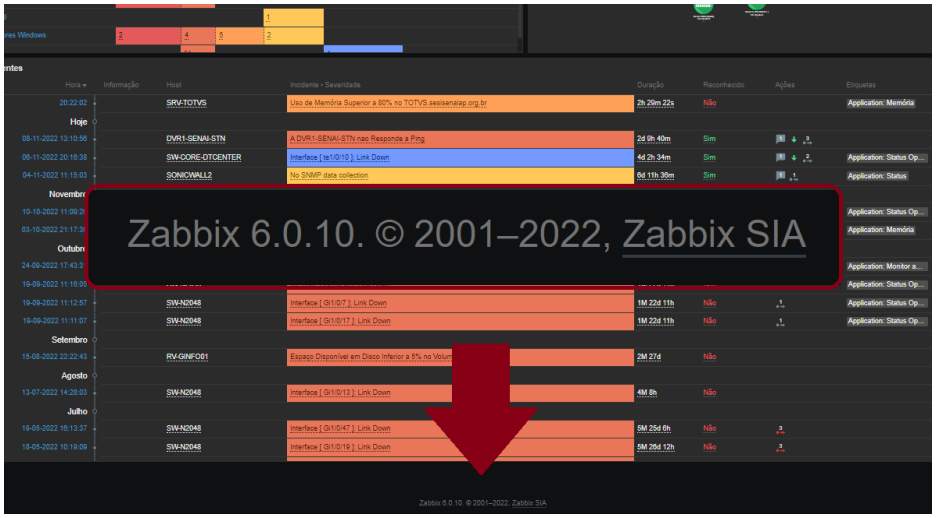
Figura 17 - Página inicial do serviço *Zabbix*.

Fonte: Autores.

Essa figura acima é a página inicial do *Zabbix* quando se conecta a ele via navegador, com o objetivo de mostrar um estado geral da rede logo ao entrar no serviço, montou-se o *Dashboard* inicial desta forma.

Descendo um pouco mais a página, conforme mostrado na figura 18, é possível visualizar a versão instalada da aplicação do *Zabbix*, como na proposta no início deste estudo de caso era fazer a instalação da versão mais atual do serviço *Zabbix*, com o passar do tempo a versão 6.0 LTS foi se atualizando, e no momento da captura da figura, a versão da instalação do Zabbix já estava na versão 6.0.10, entretanto, não deixa de ser a versão mais atual em produção.

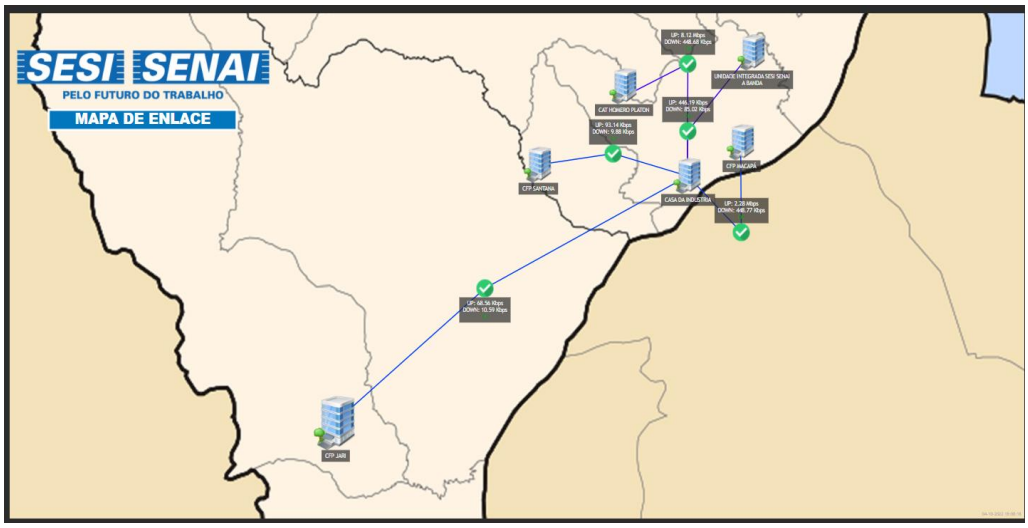
Figura 18 - Versão do serviço *Zabbix*.



Fonte: Autores.

Sobre o objetivo de monitorar os enlaces de dados de conexão das unidades do SESI SENAI pelo Amapá, foi reaproveitado a base de um mapa de monitoramento que estava no banco de dados antigo, o mesmo estava desatualizado e inoperante visto a evolução da rede do SESI SENAI com o passar do tempo. No mapa, foram atualizados os dados dos *hosts* monitorados e os *links* foram refeitos, o mapa era estático, então não mostrava os status de conexão, agora, assim como o mapa de *switches*, o mapa é ativo e relata visualmente algum erro ocorrendo no *link*. Segue adiante na figura 19, o mapa de monitoramento de enlaces.

Figura 19 - Mapa de Enlaces do SESI SENAI DR - AP.

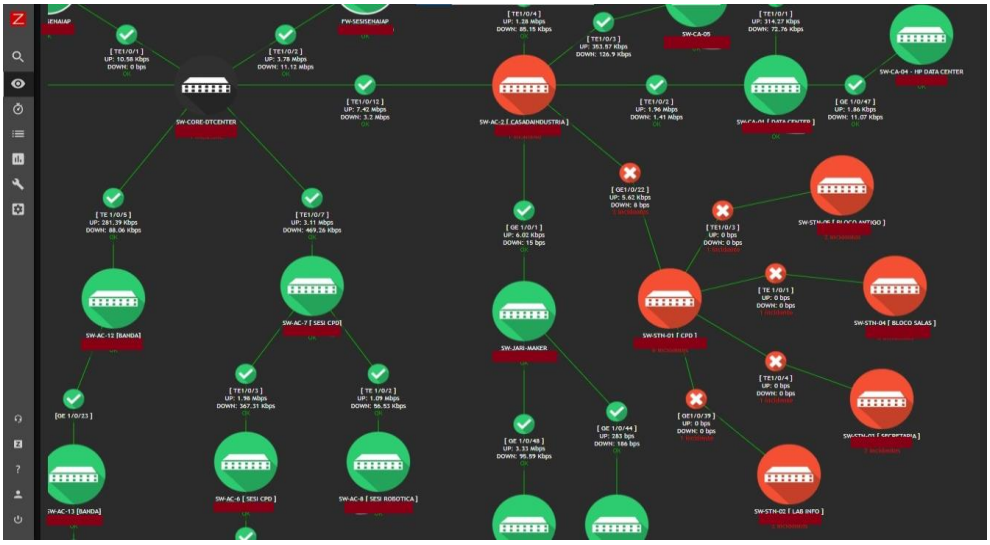


Fonte: Autores.

Em resposta ao objetivo de monitoramento dos *Switches* na rede do SESI SENAI AP, foi criado um mapa onde pode-se verificar todos os Switches Gerenciáveis sendo monitorados através de forma dinâmica. Esse modo se caracteriza pela visualização ativa de status dos equipamentos, ficando dessa forma: Caso o equipamento apresente falhas, o ícone do *Switch* se destaca e muda de cor para vermelho demonstrando falha, após a resolução do problema e o equipamento se recuperar da falha, o ícone retorna a cor verde indicando operabilidade e conexão com o equipamento.

O cenário descrito acima é exemplificado nas figuras abaixo retiradas das telas de monitoramento do SESI SENAI DR - AP, onde na figura 20 é demonstrado um cenário de *Switches* com falha e na figura 21 é demonstrado a recuperação da falha.

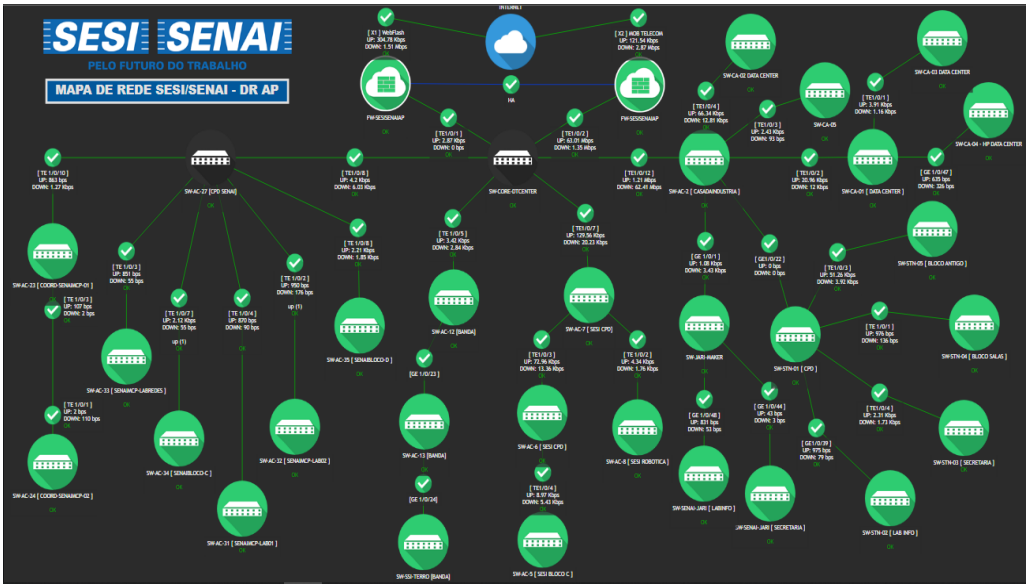
Figura 20 - Mapa de rede demonstrando falha.



Fonte: Autores.

Na figura acima é relatado um incidente ocorrido nos *Switches* da unidade do SESI SENAI - Santana, nessa ocasião, ocorreu uma falta de energia na unidade causando o desligamento dos *Switches* assim alarmando o servidor *Zabbix* da intermitência de comunicação com os *Switches.*

Figura 21 - Mapa de rede com falha corrigida.



Fonte: Autores.

Como dito anteriormente, na figura 21 é demonstrado a recuperação da falha ocorrida na figura 20. Depois que a energia foi restabelecida, os *Switches* ligaram e conseguiram se

comunicar com o servidor *Zabbix*, assim restaurando a conexão com o servidor possibilitando a visualização, no mapa, da disponibilidade dos *Switches*.

Na figura 22 é possível visualizar a lista de *hosts* criados e configurados. É demonstrado os *hosts* ativos em operabilidade, alguns inoperantes e outros com falha de comunicação. A forma de disponibilidade do *host* pode ser identificada na terceira coluna (Disponibilidade) após a identificação por IP. Os *hosts* ativos com operabilidade são identificados com o preenchimento do ícone em verde, os hosts ativos inoperantes, são identificados pela falta de preenchimento do ícone ficando com a caixinha vazia, e os hosts ativos com alguma falha de comunicação é identificado pelo preenchimento em vermelho do ícone.

Figura 22 - Lista de *hosts* cadastrados.

Fonte: Autores.

Além do preenchimento, este ícone identifica a forma de comunicação que está sendo utilizada para realizar a coleta de dados do equipamento. Podendo estar descrito como “ZBX” identificando-o como um *host* que utiliza o agente *Zabbix* como meio de comunicação ou pode estar descrito como “SNMP” identificando-o como um *host* que utiliza o protocolo de monitoramento SNMP se comunicar com o servidor *Zabbix*.

9 CONCLUSÃO E TRABALHOS FUTUROS

9.1 Conclusão

De forma conclusiva, em relação à justificativa e aos objetivos deste estudo de caso, a ferramenta *Zabbix* conseguiu exercer o seu papel como desejado pelos autores deste trabalho e pelo departamento de T.I do SESI SENAI DR - AP, atendendo a demanda que havia em identificar e relatar os problemas ocorridos de forma rápida para ajudar a equipe de T.I no gerenciamento da infraestrutura de rede.

O *Zabbix* mostrou ser um serviço indispensável em uma rede de computadores, de forma visual, ele exibe os equipamentos monitorados, por meios de agentes *Zabbix* ou protocolo SNMP, em mapas, gráficos e dashboards facilitando a análise e processo de decisão da equipe em relação a algum problema, serviço ou mudança nos equipamentos de rede.

Além disso, com base nos testes realizados, nota-se que é possível compreender muito bem o funcionamento da rede com aplicação do modelo de gerenciamento FCAPS, por coletar informações precisas sobre o funcionamento dos equipamentos e evidenciar falhas ocorridas nos componentes em tempo hábil. Isso possibilita que o responsável pela rede tome decisões rapidamente e minimize a indisponibilidade nos computadores e serviços para o usuário final.

Portanto, perante todo o processo do estudo de caso, desde o estudo da rede até o momento da elaboração dos mapas com o *Zabbix* instalado e funcional, conclui-se que a solução *Zabbix* consegue monitorar o ambiente do SESI SENAI DR - AP emitindo alertas sobre os incidentes ocorridos na rede de computadores, colaborando com a proatividade da equipe de T.I no restabelecimento dos serviços que apresentem falhas, assim ajudando no gerenciamento dos equipamentos da infraestrutura de rede.

9.2 Trabalhos futuros

Em projetos idealizados para trabalhos futuros no *Zabbix* do SESI SENAI DR - AP, objetifica estes itens abaixo:

- Buscar utilizar da ferramenta de monitoramento de SLA a fim de realizar o monitoramento de SLA do serviço de internet e outros serviços com possibilidade de fazer este monitoramento.

- Realizar a instalação de um *Zabbix proxy* para fazer o monitoramento dos servidores em hospedagens remotas.
- Utilizar a ferramenta de monitoramento *web* para monitorar a disponibilidade dos sites da empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, F. R.; PIRES, H. D. **Gerência de Redes**. Trabalho apresentado na Disciplina de Redes de Computadores I, Departamento de Engenharia de Telecomunicações, Universidade Federal Fluminense, 2004. Disponível em: http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf. Acesso em: 01 ago. 2022.

BAHLS, A. **Monitoramento Proativo do Ambiente de Rede Utilizando o Software Zabbix**. Trabalho de Conclusão de Curso, Universidade Tecnológica Federal do Paraná. Ponta Grossa, 2016. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/16765/4/PG_COADS_2016_1_01.pdf. Acesso em: 21 out. 2022.

BENICIO, E. **Monitoramento e Gerenciamento de Redes utilizando Zabbix. Trabalho apresentado ao Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal,** 2015. Disponível em: http://Zabbixbrasil.org/files/Monitoramento_e_Gerenciamento_de_Redes_Utilizando_Zabbix.pdf. Acesso em: 18 ago. 2022.

BUENO, E. **Monitoramento de computadores com uso de ferramentas de software livre**, 2012. Disponível em: https://riut.utfpr.edu.br/jspui/bitstream/1/19838/2/CT_CESOL_I_2012_05.pdf. Acesso em: 20 ago. 2022.

BRAGA, et *al*. **Uma Comparação dos Dados da Ferramenta Zabbix com a Percepção dos Usuários da Rede no Instituto Federal Catarinense-Campus. Porto Alegre**, 2019. Disponível em: https://sol.sbc.org.br/index.php/errc/article/view/9218/9121. Acesso em: 25 nov. 2022.

CASTRO, et *al*. **Ambiente de Rede Monitorado com CACTI**, Zabbix e THE DUDE. Juiz de fora, 2013. Disponível em: http://netlab.ice.ufjf.br/pdfs/DiegoOtavioDeSouzaCastro_FernandoCesarDeCarvalho_LucelioNatividadeMendes.pdf. Acesso em: 08 set. 2022.

CAPTERRA. **Monitoramento de rede.** Disponível em: <https://www.capterra.com.br/blog/1583/monitoramento-de-rede>. Acesso em: 23 nov. 2022.

CISCO, **Cisco Annual Internet Report (2018–2023) White Paper**. Disponível em: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Acesso em: 24 nov. 2022.

COMER, D. E. **Computer Networks and Internets**. 5 ed. New Jersey: Pearson, 2008.

DUARTE, O. C. **SNMP - Simple Network Management Protocol**. Disponível em: http://www.gta.ufrj.br/grad/11_1/snmp/. Acesso em: 13 ago. 2022.

FERNANDES, B. **Sistema de Gestão empresarial:** Como Escolher o Ideal para o seu Negócio. Disponível em: https://blog.softensistemas.com.br/sistemas-de-gestao-empresarial/. Acesso em: 23 ago. 2022.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. Ed. Porto Alegre: AMGH, 2010.

GIL, A.C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GIL, A.C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

JÚNIOR, J. H. T. et *al*. **Redes de Computadores**: Serviços, Administração e Segurança. São Paulo: Makron Books, 1999.

KHARB, L. **Performance Analytics of Network Monitoring Tools.** Disponível em: https://www.researchgate.net/publication/348325775_Performance_Analytics_of_Network_Monitoring_Tools. Acesso em: 24 nov. 2022.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: Uma abordagem Top-down. 3. ed. São Paulo: Addison Wesley. 2006.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet:** Uma Abordagem Top-Down. São Paulo: Addison Wesley, 2010.

KUROSE, J. F. **Redes de computadores e a Internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

NETSUPPORT, **Monitoramento de rede**. Disponível em: https://netsupport.com.br/monitoramento-de-rede/. Acessado em 23 nov. 2022.

NETWORK, K. N. **Monitoramento de rede**. Disponível em: https://network-king.net/pt-pt/ferramentas-de-monitoramento-de-rede/. Acessado em 23 nov. 2022.

ORACLE, MYSQL. **Documentation**. Disponível em: https://dev.mysql.com/doc/refman/8.0/en/rebuilding-tables.html. Acesso em: 08 set. 2022.

PEREIRA, S. **Metodologia da pesquisa científica**. 1. ed. Santa Maria, UFSM, NTE, 2018.

RAUPP, M.; BEUREN, M. **Metodologia da pesquisa aplicável às ciências sociais**. Como elaborar trabalhos monográficos em contabilidade: teoria e prática. São Paulo, 2012. Disponível em: http://www.geocities.ws/cienciascontabeisfecea/estagio/Cap_3_Como_Elaborar.pdf. Acesso em: 24 set. 2022.

RIBEIRO, T. **Fundamentos de redes de computadores**. 1. Ed. Londrina: Editora e Distribuidora Educacional S.A, 2016.

ROCHA, A. **O que é SNMP e qual a importância deste protocolo?** Opservices, Porto Alegre, 19 de jun. de 2017. Disponível em: https://www.opservices.com.br/snmp/. Acesso em: 13 ago. 2022.

RODRIGUES, R. **Instalação do Zabbix 6 em 3 camadas**. YouTube, 23 de set. de 2022. Disponível em: https://www.youtube.com/watch?v=7kVwUbhm_BA. Acesso em: 24 set. 2022.

SANTOS, M. A. B; BARROS, R. C. **Direções no monitoramento em redes de larga escala**: Uma visão geral, ferramentas e tendências. Disponível em:

https://www.editorarealize.com.br/editora/anais/conidis/2016/TRABALHO_EV064_MD1_SA6_ID2261_20102016121118.pdf. Acesso em: 23 de nov. 2022.

SCAPIN, A. H. **Análise de ferramentas de gerência de redes e interfaces web**. Disponível em: https://www.ufsm.br/app/uploads/sites/495/2019/05/2015-Alex-Scapin.pdf. Acesso em: 24 nov. 2022.

SAYDAM, T. **From Networks and Network Management into Service and Service Management.** 4 ed. Journal of Networks and System Management, 1996.

SIMÕES, J. M. **Monitorização automática de redes de computadores**: estudo e proposta de uma nova solução. Lisboa, 2010. Disponível em: https://run.unl.pt/handle/10362/5049?locale=en. Acesso em: 25 set. 2022.

SILVA, R. Live - **Tudo sobre a instalação do Zabbix**. Youtube, 19 de julho de 2021. Disponível em: https://www.youtube.com/watch?v=jdHo7yefiMg&t=415s. Acesso em: 02 ago. 2022.

STORCH, M. S. **Uma arquitetura para gerência de rede de máquinas virtuais com ênfase na emulação de sistemas distribuídos**. Dissertação de Mestrado. Rio Grande do Sul, 2008. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/5033/1/407650.pdf. Acesso em: 18 ago. 2022.

TANENBAUM, A. S. WETHERALL, D. (2011) **Redes de Computadores**. São Paulo: Pearson Prentice Hall.

TELECO, **Gerenciamento e Monitoramento de Rede 1, Teoria de Gerência de Redes**. Disponível em: https://www.teleco.com.br/tutoriais/tutorialgmredes1/pagina_3.asp. Acesso em: 05 ago. 2022.

TEODORO, S. M. **Gerência de redes com Zabbix**. 2013. 51 f. Trabalho de Conclusão de Curso, Faculdade de Tecnologia de Americana. Disponível em:http://ric.cps.sp.gov.br/bitstream/123456789/1190/1/20131S_SILVAMarcosTeodoroda_TCCPD1208.pdf. São Paulo - Americana, 2013. Acesso em: 21 out. 2022.

VARGAS, D. P. **Gerenciamento e monitoramento de redes**: um estudo de caso da utilização da ferramenta Zabbix no âmbito da base administrativa da guarnição de Santa Maria. 2020. Disponível em: https://bdex.eb.mil.br/jspui/handle/123456789/7928. Acesso em: 02 set. 2022.

SIA, Z. Zabbix, **Documentation**. Disponível em: https://www.Zabbix.com/documentation/6.0/pt/manual. Acesso em: 11 de set. 2022.

SIA, Z. Zabbix, **Fórum**. Disponível em: https://www.Zabbix.com/forum/em-portugues-y-en-espanol/447535-exportar-importar-banco-de-dados-em-uma-nova-instala%C3%A7%C3%A3o. Acesso em: 7 set. 2022.

.

SILVA, R. **Arquitetura de instalação do Zabbix**. YouTube, 28 de Jul. de 2021. Disponível em: https://www.youtube.com/watch?v=AS1iBFfgiaE. Acesso em: 14 ago. 2022.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**. 5ª ed. Rio de Janeiro: Campus, 2005.

ANEXO A – CONFIGURAÇÃO

Esse anexo contém o passo a passo executado em ambiente de produção referente à instalação dos servidores que compõem o serviço Zabbix.

1 Servidor de Banco de Dados

Comentário referente ao comando	Comando Linux
Atualização da lista de pacotes	apt update && apt upgrade -y
Ajuste de time zone	timedatectl set-timezone America/Belem
Instalar um NDP para sempre corrigir a hora	apt-get install -y chrony
Definir início do Chrony junto ao início da máquina	systemctl enable --now chrony
Instalar utilitários para o servidor de Banco de Dados	apt-get install -y net-tools nano wget curl tcpdump vim nmap mariadb-server
iniciar o MARIADB e habilitá-lo para iniciar junto a máquina	systemctl enable --now mariadb
Agora vamos iniciar o script que ajuda na pós instalação do server mariadb	mysql_secure_installation
Preencher	Enter current password for root (enter for none): (em branco) Set root password? [Y/n] y New password: (defina uma senha para o usuário root do banco de dados) Remove anonymous users? [Y/n] y Disallow root login remotely? [Y/n] y Remove test database and access to it? [Y/n] y Reload privilege tables now? [Y/n] y
Acessar o mysql	mysql -u root -p (senha que definiu para o usuário root do db)
Criação de banco de dados zabbix	CREATE DATABASE zabbixdb CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
Criação do usuário zabbix e sua senha	CREATE USER 'zabbix'@'endereço ip do servidor do zabbix' IDENTIFIED BY 'password';
Garantir privilégios do banco de dados zabbix ao usuário zabbix	GRANT ALL PRIVILEGES ON zabbixdb.* to zabbix@endereço ip do servidor do zabbix identified by ‘password';
Criação do usuário para o front-end e sua senha	CREATE USER 'front-end'@'endereço ip do front-end' IDENTIFIED BY 'password';

Garantir privilégios do banco de dados zabbix ao usuário do front-end	GRANT ALL PRIVILEGES ON zabbixdb.* to front-end@endereço ip do front-end identified by ‘password';
Atualização dos privilégios	FLUSH PRIVILEGES;
Abrir conexão para o mariadb	nano /etc/mysql/mariadb.conf.d/50-server.cnf
Altere o campo	bind-address = 0.0.0.0
Definir início do mysql junto ao início da máquina	systemctl enable –now mariadb.service
Reinicie o serviço do mariadb	systemctl restart mariadb.service

2 Servidor de Aplicação Zabbix

Comentário referente ao comando	Comando Linux
Atualização da lista de pacotes	apt update && apt upgrade -y
Ajuste de time zone	timedatectl set-timezone America/Belem
Instalar um NDP para sempre corrigir a hora	apt-get install -y chrony
Definir início do chrony junto ao início da máquina	systemctl enable --now chrony
Instalar utilitários para o servidor zabbix	apt-get install -y net-tools nano wget curl tcpdump vim nmap policycoreutils-python-utils snmp mariadb-client
Criação o diretório /installzbx	mkdir /home/installzbx
Entre no diretório /installzbx	cd /home/installzbx
Realização do download do zabbix	wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-3%2Bubuntu22.04_all.deb
	dpkg -i zabbix-release_6.0-3+ubuntu22.04_all.deb
Atualização da lista de pacotes do repositório e upgrade dos pacotes do sistema	apt update && apt upgrade -y

Instalação de ferramentas para servidor zabbix	apt-get install -y zabbix-agent2 zabbix-server-mysql zabbix-sql-scripts
Editar o arquivo de configuração do server zabbix para dizer que ele irá usar um banco de dados que não está no localhost	nano /etc/zabbix/zabbix_server.conf
Altere as linhas	DBHost= (endereço do servidor DB) DBName= (nome do database definido no comando 'CREATE #DATABASE "nome do db" .....') DBUser= (user do db para o zabbix) DBPassword= (senha do usuário zabbix para o banco de dados do zabbix) CacheSize= para 64M (ou mais, conforme a necessidade)
Configuração do agent zabbix	nano etc/zabbix/zabbix_agent2.conf
Altere as linhas	“passive check” Server= (servidor zabbix que vai fazer a coleta de dados) “ServerActive” Server= (servidor zabbix que vai fazer a coleta de dados) Hostname: (hostname do servidor que está sendo instalado o agent zabbix) StartAgents=5 (descomentar) Timeout=3 (descomentar)
Iniciar agente zabbix e zabbix server	systemctl start zabbix-server zabbix-agent2
Definir início do agente zabbix e do servidor zabbix junto ao início da máquina	systemctl enable --now zabbix-server zabbix-agent2
Com os pacotes do zabbix server já instalados, popule a base de dados do banco de dados	zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -u(usuário correspondente ao zabbix no db) -p(senha definida para o usuário)-h (ip do servidor banco de dados)

3 Servidor Web

Comentário referente ao comando	Comando Linux
Atualização da lista de pacotes	apt update && apt upgrade -y
Ajuste de time zone	timedatectl set-timezone America/Belem
Instalar um NDP para sempre corrigir a hora	apt-get install -y chrony
Definir início do chrony junto ao início da máquina	systemctl enable --now chrony

Instalar utilitários para o servidor web	apt-get install -y net-tools nano wget curl tcpdump vim nmap zabbix-front-end-php php8.1-mysql nginx
reinicie o servidor	reboot
Criação o diretório /installzbx	mkdir /home/installzbx
Entre no diretório /installzbx	cd /home/installzbx
Fazer download dos pacotes .deb do zabbix	wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-3%2Bubuntu22.04_all.deb
	dpkg -i zabbix-release_6.0-3+ubuntu22.04_all.deb
Atualização da lista de pacotes do repositório e upgrade dos pacotes do sistema	apt update && apt upgrade -y
Instalando os pacotes necessários para o nginx	apt-get install -y zabbix-nginx-conf zabbix-web-service
No front-end temos que configurar o arquivo referente ao virtual host do zabbix	nano /etc/nginx/conf.d/zabbix.conf
Alterar as linhas referentes tirando os # e alterando os campos	listen 80;
	server_name 192.168.54.9;
Iniciar o nginx	systemctl start nginx
Definir início do servidor web junto ao início da máquina	systemctl enable –now nginx
Acessando zabbix web pelo endereço IP no navegador e configurando os campos	Database server details Database type: MySQL Database Host: ip do servidor web Database port: 0 default Database name: zabbixdb User: front-end (usuário do front-end criado no db para acessar o db do zabbix pelo nginx) Password: (senha definida para o usuário do front-end no banco de dados) Zabbix server details Host: (ip do host zabbix server app) Port: 10051 Name: Zabbix (opcional)

ANEXO B - TERMO DE AUTORIZAÇÃO

SESI SENAI DR – AP

COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

DEPARTAMENTO DE TI DO SESI SENAI DR - AP

TERMO DE AUTORIZAÇÃO PARA DIVUGAÇÃO DE INFORMAÇÕES DA REDE DE COMPUTADORES DO SESI SENAI DR - AP

Razão Social: Serviço Social da Indústria Inscrição Estadual: _____

Endereço Completo: Rua Leopoldo Machado, 2349

Nome do Responsável: Ernesto Gomes P. Júnior Função: Coordenador TI

Telefone: (96) 981237608 e-mail: ernesto.gomes@sesisenai.org.br

Tipo de produção intelectual: ( ) Monografia; (X) TCC; ( ) Relatório de estágio;

( ) Dissertação; ( ) Tese; ( ) Outro: _____

Título/Subtítulo: Estudo de caso no SESI SENAI DR - AP: Implementação da ferramenta Zabbix na versão 6.0 LTS para monitoramento dos equipamentos de rede.

Autor: Isabelly Costa de Abreu Código de Matrícula: 2019110110005

Autor: Kayuã Kayo Mariano Rodrigues Barbosa Código de Matrícula: 2019110110039

Nome do Curso: Tecnólogo em Redes de Computadores

Campus: Instituto Federal de Educação, Ciência e Tecnologia do Amapá – Campus Macapá.

Como representante da empresa acima nomeada, declaro que as informações e/ou documentos disponibilizados pela empresa para o trabalho citato:

(X) Podem ser Publicados sem restrição.

( ) Possuem restrição parcial por período _____ anos, não podendo ser publicadas as seguintes informações e/ou documentos:

_____

_____

( ) Possuem restrição total para publicação por período de _____ anos, pelos seguintes motivos:

_____

_____

Ernesto Gomes P. Júnior

Representante do Departamento

Macapá, 13 de dezembro de 2022

Local e Data

Ernesto Gomes P. Júnior
Coordenador de Tecnologia da Informação-CTIC
SESI-SENAI-DR/AP