UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ANDERSON CHAVES
RAUL SALES C. VIEIRA

IMPLANTAÇÃO DE UMA SOLUÇÃO OPEN SOURCE NA GESTÃO DE UMA REDE DE COMPUTADORES EM UMA MÉDIA EMPRESA COM AS FERRAMENTAS ZABBIX E GRAFANA

Maceió
2020

ANDERSON CHAVES
RAUL SALES C. VIEIRA

IMPLANTAÇÃO DE UMA SOLUÇÃO OPEN SOURCE NA GESTÃO DE UMA REDE DE COMPUTADORES EM UMA MÉDIA EMPRESA COM AS FERRAMENTAS ZABBIX E GRAFANA

Trabalho de Conclusão de Curso submetido ao Curso de Sistemas de Informação do Instituto de Computação da Universidade Federal de Alagoas como requisito parcial para a obtenção do Grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Almir Pereira Guimarães

Maceió
2020

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 - 1767

C512i Chaves, Anderson.

Implantação de uma solução *open source* na gestão de uma rede de computadores em uma média empresa com as ferramentas Zabbix e Grafana / Anderson Chaves, Raul Sales C. Vieira. – 2021.

64 f. : il.

Orientador: Almir Pereira Guimarães.

Monografia (Trabalho de conclusão de curso em Sistemas de Informação) – Universidade Aberta do Brasil. Universidade Federal de Alagoas, Instituto de Computação. Maceió, 2020.

Bibliografia: f. 59-64.

1. Redes de computadores - Gerência. 2. Zabbix (*Software*). 3. Grafana (*Software*). 4. *Simple Network Management Protocol* (Protocolo de Rede de Computador). 5. *Management Information Base* (Base de Informações de Gerenciamento). I. Vieira, Raul Sales C. II. Título.

CDU: 004.7

ANDERSON CHAVES
RAUL SALES CANSANÇÃO VIEIRA

IMPLANTAÇÃO DE UMA SOLUÇÃO OPEN SOURCE NA GESTÃO DE UMA REDE DE COMPUTADORES EM UMA MÉDIA EMPRESA COM AS FERRAMENTAS ZABBIX E GRAFANA..

Este Trabalho de Conclusão de Curso (TCC) foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo Instituto de Computação da Universidade Federal de Alagoas.

Maceió, _10_ de __dezembro_ de 2020.

Prof. PETRÚCIO ANTÔNIO MEDEIROS BARROS, Me.
Coordenador do Curso de Sistemas de Informação

Banca Examinadora:

Prof. ALMIR PEREIRA GUIMARÃES, Dr. (Orientador)
Universidade Federal de Alagoas
Instituto de Computação

Prof. PETRÚCIO ANTÔNIO MEDEIROS BARROS, Me.
Universidade Federal de Alagoas
Instituto de Computação

Prof. RÔMULO OLIVEIRA, Me.
Universidade Federal de Alagoas
Campus Arapiraca

AGRADECIMENTOS

Agradecemos aos nossos familiares que nos apoiaram até aqui e que foram a nossa fonte de inspiração e entenderam nossos momentos de ausência durante essa caminhada de anos. Somos gratos aos colegas de Faculdade que lutaram junto conosco todos os dias. Aos amigos que não deixaram o cansaço nos vencer e sempre nos incentivaram a não desistir. Aos nossos mestres que acompanharam toda a nossa trajetória dentro do curso Sistemas de Informação. Ao nosso orientador professor Almir Pereira Guimarães que foi incansável em suas orientações, pesquisas e revisões. Nosso muito obrigado à Universidade Federal de Alagoas por nos proporcionar o melhor ambiente educacional. Agradecemos à Deus que nos deu força e nos permitiu realizar esse sonho.

RESUMO

As redes de computadores nas últimas décadas tornaram-se um elemento de importância fundamental e vital para qualquer órgão ou empresa. É indispensável que a infraestrutura destas redes apresente requisitos de confiabilidade, segurança e desempenho de maneira satisfatória, a fim de de oferecer suporte total às aplicações críticas para o bom funcionamento dos processos envolvidos nas organizações públicas ou privadas.

Diante desse cenário, o monitoramento da rede é um serviço fundamental para obter uma resposta rápida e precisa sobre o funcionamento da infraestrutura computacional presente. Uma rede é o coração de uma infraestrutura de Informática, de maneira que quando uma rede falha, o fluxo de informações necessárias para os aplicativos e operações de negócios é interrompido.

Levando em consideração todos esses pontos, a proposta deste trabalho é a implantação de um sistema de monitoramento de redes de computadores, integrado a um painel visual, permitindo a visão de informações centralizadas, que serão obtidas para a tomada de decisões assertivas e imediatas, com o objetivo de manter a sustentação dos serviços das redes de computadores de uma empresa na área de saúde.

O sistema de gerenciamento utilizado neste trabalho foi o Zabbix, que é um *software* de código aberto que permite o monitoramento de todos os recursos de uma infraestrutura de informática, garantindo a manutenção de sua integridade, disponibilidade e desempenho. Para exibir as informações colhidas pelo Zabbix, foi utilizado o Grafana que também é uma plataforma de código aberto para monitoramento, análise e visualização de dados.

De uma maneira geral, a solução integrada das duas ferramentas se mostrou bastante eficiente, dando à equipe de informática, proatividade na resolução de problemas, deixando-os quase sempre, transparentes aos colaboradores. Além disso, as ferramentas contribuíram de forma satisfatória na solução de dois problemas propostos neste trabalho. Foram eles: o cuidado com o espaço disponível em disco nos servidores de imagens de exames, a fim de evitar a interrupção na realização dos exames; bem como auxiliando a gestão de informática, através da possibilidade de elaboração de relatórios técnicos detalhados.

Palavras-chaves: Gerenciamento de Redes; Zabbix; Grafana; SNMP; MIB.

ABSTRACT

Computer networks in recent decades have become an element of fundamental and vital importance for any organ or company. It is essential that the infrastructure of these networks present requirements for reliability, security and performance in a satisfactory manner, in order to offer full support to applications critical to the proper functioning of the processes involved in public or private organizations.

In view of this scenario, network monitoring is a fundamental service to obtain a quick and accurate response on the functioning of the present computational infrastructure. A network is the heart of an IT infrastructure, in a way that when a network fails, the flow of information necessary for applications and business operations is interrupted.

Taking into account all these points, the purpose of this work is the implementation of a computer network monitoring system, integrated with a visual panel, allowing the centralized information view, which will be obtained for assertive and immediate decisions , in order to maintain the sustainability of a company's computer network services in the health area.

The management system used in this work was Zabbix, which is open source software that allows the monitoring of all the resources of an IT infrastructure, ensuring the maintenance of its integrity, availability and performance. To display the information collected by Zabbix, Grafana was used, which is also an open source platform for monitoring, analyzing and visualizing data.

In general, the integrated solution of the two tools proved to be very efficient, giving the IT team proactivity in solving problems, making them almost always transparent to employees. In addition, the tools contributed satisfactorily to the solution of two problems posed in this work. They were: the care with the available disk space in the exam image servers, in order to avoid interruption in the exams; as well as assisting computer management, through the possibility of preparing detailed technical reports.

Keywords: Network Management, Zabbix; Grafana; SNMP; MIB.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

- **DNS** - Sistemas de Domínios de Nome. Sigla proveniente do inglês *Domain Name System*.
- **ERP** - Software de gestão para empresas, que significa Planejamento dos Recursos da Empresa. Sigla proveniente do inglês *Enterprise Resource Planning*.
- **FAB** - Força Aérea Brasileira.
- **HTTP** - Protocolo de Transferência de Hipertexto. Sigla proveniente do inglês *Hypertext Transfer Protocol*.
- **ICMP** - Protocolo de Mensagens de Controle de Internet. Sigla proveniente do inglês *Internet Control Message Protocol*.
- **IMAP** - Protocolo de Acesso a Mensagem da Internet. Sigla proveniente do inglês *Internet Message Access Protocol*.
- **IOS** - *Software* usado na maioria dos roteadores e atuais *switches* de rede da Cisco Systems. Sigla proveniente do inglês *Internetwork Operating System*.
- **IPMI** - Interface Inteligente de Gerenciamento de Plataforma. Sigla proveniente do inglês *Intelligent Platform Management Interface*.
- **JSON** - Notação de Objetos JavaScript. Sigla proveniente do inglês *JavaScript Object Notation*.
- **LDAP** - Protocolo Leve de Acesso ao Diretório. Sigla proveniente do inglês *Lightweight Directory Access Protocol*.
- **MIB** - Base de Informações de Gerenciamento. Sigla proveniente do inglês *Management information base*.
- **MPLS** - Comutação de Rótulos Multiprotocolo. Sigla proveniente do inglês *Multi Protocol Label Switching*.
- **NBR** - Norma Brasileira. Conjunto de normas e regras técnicas relacionadas a documentos, procedimentos ou processos aplicados a empresas ou determinadas situações
- **OID** - Identificador de Objeto. Sigla proveniente do inglês *Object Identifier*.
- **OSI** - Interconexão do Sistema Aberto. Sigla proveniente o inglês *Open System Interconnection*.
- **POP** - Protocolo de Correio. Sigla proveniente do inglês *Post Office Protocol*.

- **RFC** - Pedido Para Comentários. Sigla proveniente do inglês *Request for Comments*.
- **SISU** - Sistema de Seleção Unificada. Programa do Ministério da Educação (MEC) que oferece vagas em universidades públicas sem precisar fazer o vestibular.
- **SLA** - Acordo de Nível de Serviço. Sigla proveniente do inglês *Service Level Agreement*.
- **SMS** - Serviço de mensagens curtas. Sigla proveniente o inglês *Short Message Service*.
- **SMTP** - Protocolo Simples de Transferência de Correio. Sigla proveniente do inglês *Simple Mail Transfer Protocol*.
- **SNMP** - Protocolo Simples de Gerência de Rede. Sigla proveniente do inglês *Simple Network Management Protocol*.
- **TCP** - Protocolo de Controle de Transmissão. Sigla proveniente do inglês *Transmission Control Protocol*.
- **TIC** - Tecnologias da Informação e Comunicação.
- **UDP** - Protocolo de Datagrama do Usuário. Sigla proveniente do inglês *User Datagram Protocol*.
- **USM** - Modelo de segurança baseado no usuário. Sigla proveniente do inglês *User-based Security Model*.
- **VACM** - Modelo de Controle de Acesso baseado em Visualização. Sigla proveniente do inglês *View-based Access Control Model*.
- **VPN** - Rede Privada Virtual. Sigla proveniente do inglês *Virtual Private Network*.

SUMÁRIO

CAPÍTULO 1 – INTRODUÇÃO

1.1 Visão Geral

No princípio das redes de computadores, quando estas representavam apenas temas de pesquisa e estudo e não possuíam o uso maciço por milhões de pessoas dos dias atuais, a expressão “gerenciamento de rede” não era uma preocupação de que se pudesse ouvir falar. Testes elementares, a exemplo do *ping* eram suficientes para identificar a origem de um problema na rede, o que já possibilitava a sua devida manutenção (KUROSE, 2010).

Esse cenário mudou drasticamente com o exponencial crescimento dessa grande rede, chamada *Internet* pública, bem como das redes privadas, que, saindo de pequenas redes, alcançaram o estágio de infraestruturas globais, tornando importante o efetivo gerenciamento da sua grande quantidade de itens de *hardware* e *software* (KUROSE, 2010).

Hoje, as redes estão presentes não apenas nas mais diversas organizações, mas também em nossos lares, onde é cada vez mais presente o compartilhamento de informações, além do hábito de assistir filmes, ouvir músicas, jogar e conversar com amigos através de chamadas telefônicas e videotelefônicas (TANENBAUM, 2003).

Seu crescimento facilitou a comunicação e o acesso à informação de governos, empresas, escolas e outras instituições, tornando seus trabalhos mais eficientes e ágeis.

A adoção de redes também proporciona economia. Segundo Tanenbaum (2003), "Em termos um pouco mais genéricos, a questão aqui é o compartilhamento de recursos, e o objetivo é tornar todos os programas, equipamentos e especialmente dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso e do usuário".

Um exemplo comumente utilizado, é o compartilhamento de uma impressora para um grupo de funcionários, onde não é necessário que cada um deles tenha uma impressora particular, facilitando em casos de manutenção, onde será necessário concentrar esforços em apenas um equipamento e não em um conjunto deles (TANENBAUM, 2003).

Desta forma, monitorar estas redes a fim de evitar falhas e indisponibilidades, assim resguardando a segurança da informação, tornou-se tão essencial quanto a sua criação, uma vez que a segurança da informação se mostra cada vez mais necessária nas empresas, pois ela tornou-se um ativo de grande valor (TECJUMP, 2017). Segundo Gonçalves (2000), "se não existissem preocupações com risco de segurança relativos à conectividade na Internet, não haveria necessidade de *firewalls* e nem de outros mecanismos de defesa".

De acordo com Tanenbaum (2003), "organizações com centenas de escritórios dispersos por uma extensa área geográfica podem, com um simples apertar de um botão, examinar o status atual de suas filiais mais remotas". E ainda, "à medida que cresce nossa capacidade de colher, processar e distribuir informações, torna-se ainda maior a demanda por formas de processamento de informações ainda mais sofisticadas". Assim, as ferramentas de monitoramento têm um potencial muito grande para contribuir com o negócio das empresas.

O monitoramento da estrutura de rede não deve limitar-se à premissa de um serviço estar respondendo ou não, ou se um determinado equipamento está ligado ou não. O que se deve ter em mente é que tanto falhas de *hardware* como falhas de *software* podem produzir efeitos desastrosos no ambiente de rede, onde o gerente de rede deve manter a preocupação de que precisa monitorar ambos (COMER, 2008).

Uma situação que deve ser considerada ao se planejar uma estrutura de rede e seu monitoramento, é que diversos dispositivos empregados são criados para lidar com problemas e resolvê-los automaticamente. Exemplo disso são os protocolos de rede, a citar, o TCP, que desconsidera as falhas de pacotes, limitando-se a retransmitir os que apresentem falha, o que gera o potencial despercebimento de perda intermitente de pacotes pelo administrador de rede, comprometendo assim, a largura de banda da estrutura de rede (COMER, 2008).

A confiabilidade e a disponibilidade são métricas relacionadas à probabilidade de falha na rede (AMARAL, 2014). Falando em disponibilidade e analisando as redes de computadores, o que se espera é que um serviço esteja sempre ativo, pronto para uso e atenda o usuário no momento da sua solicitação. A disponibilidade, em conjunto com a confiabilidade são requisitos básicos para a segurança da informação. Segundo a NBR 5462-94 da ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS), disponibilidade é:

> Capacidade de um item estar em condições de executar uma certa função em um dado instante ou durante um intervalo de tempo determinado, levando-se em conta os aspectos combinados de sua confiabilidade, mantenabilidade e suporte de manutenção, supondo que os recursos externos requeridos estejam assegurados.

Ainda, a mesma NBR 5462 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 1994, p. 3), define confiabilidade como “Capacidade de um item desempenhar uma função requerida sob condições especificadas, durante um dado intervalo de tempo”.

Assim, objetivando o correto planejamento e crescimento de redes estruturadas, além de monitorar e oferecer uma alta disponibilidade de seus recursos, vem a necessidade de se gerenciar estas redes (BUENO, 2012). Conforme Comer (2015), com o seu exponencial aumento, cada vez mais torna-se complexo e árduo que o gerenciamento dessas redes seja executado apenas por investidas humanas. Dessa forma então, o emprego de automatização se apresenta necessário.

Utilizando-se o Zabbix torna-se viável monitorar diversos parâmetros da infraestrutura de redes de computadores, além da saúde dos serviços. Sua estrutura de notificação aceita configurações de alertas para praticamente qualquer evento, ocasionando uma acelerada reação para empecilhos exibidos (ZABBIX SIA, 2018).

Por intermédio de sua *interface web*, é possível observar o estado da rede, bem como a saúde de seus servidores remotamente. Ele pode ser utilizado para o monitoramento de pequenas empresas que possuam alguns servidores, bem como de grandes corporações, com milhares de servidores (ZABBIX SIA, 2018).

O Zabbix permite tanto o monitoramento centralizado a partir do servidor Zabbix, executado em intervalos regulares (*pooling*), quanto o processamento de informações, executados pelos hosts e enviados ao Zabbix para análise (*trapping*). Com a *interface web* é possível acompanhar relatórios e estatísticas, além de revisar parâmetros de configuração (ZABBIX SIA, 2018).

A partir do contexto apresentado, o objetivo deste trabalho é o de proporcionar o monitoramento das redes de computadores de uma empresa que atua na área de saúde, a fim de manter uma alta disponibilidade destas infraestruturas de redes. Apresentando com destaque o *software* Zabbix, que segundo Zabbix Sia (2018), foi concebido como “uma solução de monitoração integrada, que provê diversos recursos de monitoração em um único pacote”, em conjunto com o Grafana.

1.2 Motivação

Mais importante que compartilhar recursos, hoje em dia é vital o tratamento e a disseminação da informação para as empresas de pequeno, médio e grande porte. Segundo Tanenbaum (2003):

> A maioria das empresas tem registros de clientes, estoques, contas a receber, extratos financeiros, informações sobre impostos e muitas outras informações *on-line*. Se todos os computadores de um banco sofressem uma pane, ele provavelmente não permaneceria com suas operações por mais de cinco minutos. Uma instalação industrial moderna, com uma linha de montagem controlada por computadores, também não permaneceria com suas operações além deste período. Hoje, até mesmo uma pequena agência de viagens ou uma firma jurídica com três pessoas depende intensamente de redes de computadores para permitir aos seus funcionários acessarem informações e documentos relevantes de forma instantânea.

A história recente mostra casos em que a falha da rede causou prejuízos tanto às empresas quanto aos seus usuários. Em 2019, por exemplo, uma falha no SISU, causada por sobrecarga de acesso, com picos de 350 mil acessos simultâneos (10 vezes a mais que o esperado), fez com que alunos não conseguissem efetuar a inscrição (G1, 2019).

Já em 2017, a empresa aérea *British Airways* enfrentou grandes falhas na área de informática que a levou a cancelar todos os voos de *Heathrow* e *Gatwick*. Foram mais de mil voos afetados, além do *CallCenter* da empresa, do *site* e do aplicativo para dispositivos móveis (JEE E MACAULAY, 2018).

O *TD Bank*, oitavo maior banco dos Estados Unidos, em fevereiro de 2018, após uma atualização mal sucedida das aplicações no servidor, acabou deixando os clientes sem acesso às suas contas *on-line* por cinco dias. Com isso, clientes frustrados, congestionaram as linhas telefônicas a fim de fazerem reclamações, gerando mais problemas e reclamações em outros meios como as redes sociais (33GIGA, 2019).

Em 2018, o hospital *Welsh NHS*, do Reino Unido, sofreu falha geral, causando a inacessibilidade de arquivos de pacientes por parte dos médicos e funcionários. A falha teria sido causada por problemas técnicos nos servidores. O hospital passou por uma grande interrupção, já que não era possível acessar resultados de exames de sangue e raios-X, nem novas informações podiam ser inseridas nos dados dos pacientes (JEE E MACAULAY, 2018).

Na *Black Friday* de 2018, cerca de 65 empresas de e-commerce tiveram um prejuízo em torno de R$ 23,9 milhões causados por instabilidades em seus sistemas devido ao grande volume de acessos, ocasionando lentidão no carregamento das páginas e mesmo ficando fora do ar por longos períodos (33GIGA, 2019).

Dados problemas dessa natureza e buscando a máxima eficiência e produtividade, o administrador precisa de ferramentas que mostrem o ativo da rede que esteja apresentando falha. Além de estarem aptas a atuar sobre os serviços ou componentes da rede, de maneira tal, por exemplo, a reiniciar um serviço que venha a parar de responder, ou ainda, emitir avisos sobre discos de armazenamento que estejam com pouco espaço disponível ou com indicativos de que irão falhar em breve (BAHALS, 2016).

Desta forma, o tema do presente trabalho foi escolhido alinhado com as atividades dos autores, que trabalham em setores de informática de empresas, que têm o foco no monitoramento da infraestrutura, a fim de resguardar a alta disponibilidade dos recursos importantes à atividade empresarial.

1.3 Objetivos

1.3.1 Objetivo geral

Implantar as ferramentas *open source* Zabbix e Grafana, a fim de incrementar o gerenciamento de redes corporativas, proporcionando um gerenciamento integrado. Zabbix e Grafana foram escolhidas devido à vivência técnica prática dos autores e por agregarem características melhoradas, além de superar pontos fracos de outras ferramentas do mercado.

1.3.2 Objetivos específicos

- Instalar e configurar o Zabbix Server versão 4.0 LTS em um servidor virtualizado, rodando o Sistema Operacional *FreeBSD* 64 bits;
- Instalar e configurar o Agente do Zabbix nos servidores a serem monitorados;
- Configurar os itens que serão monitorados e as *triggers* nos servidores que serão gerenciados, para a ativação de notificações de eventos na rede;

- Demonstrar a melhoria causada pelo monitoramento em dois pontos escolhidos a princípio pela sua criticidade, quais sejam:
    - Espaço em disco de servidores essenciais ao negócio da empresa; e
    - Identificação de pontos de melhorias na infraestrutura da rede.

1.4 Estrutura deste Trabalho

Este trabalho está estruturado da seguinte maneira. Além do capítulo introdutório, o segundo capítulo apresenta trabalhos relacionados com nossa pesquisa. O terceiro capítulo apresenta a fundamentação teórica, detalhando as áreas do gerenciamento e o que cada uma é encarregada de monitorar. Apresentando também os protocolos utilizados pelas plataformas de gerenciamento, em detalhe, o funcionamento do protocolo SNMP. No quarto capítulo são apresentadas as plataformas de gerenciamento mais conhecidas do mercado, com destaque para o detalhamento do Zabbix e Grafana, objetos de estudo deste trabalho. No capítulo quinto, é versado sobre a metodologia aplicada na elaboração deste trabalho e análise dos dados após a implantação do projeto de monitoramento. O sexto capítulo discorre sobre a implantação do gerenciamento, apresentando a infraestrutura da empresa objeto do estudo, passando pela instalação e configuração dos *softwares* necessários para o monitoramento, finalizando com o detalhamento de dois problemas que foram tratados com a implantação do processo. O sexto capítulo apresenta as considerações finais deste trabalho, focando nas contribuições proporcionadas à infraestrutura da empresa, além de apresentar sugestões de trabalhos futuros em complemento a este elaborado.

CAPÍTULO 2 - TRABALHOS RELACIONADOS

Esse capítulo detalha pesquisas que se relacionam com o tema proposto em nosso trabalho de conclusão de curso, como, também, o resultado que pretendemos alcançar com a implantação de um ambiente monitorado e controlado de redes.

Bahals (2016) diz: “O monitoramento proativo visa contribuir para a diminuição das ocorrências de indisponibilidade no ambiente de rede, uma vez que alerta o administrador do sistema sobre os locais onde poderão ocorrer falhas. Em alguns casos, atua automaticamente para o restabelecimento do serviço”. Neste trabalho, o autor conseguiu, com o Zabbix, diminuir consideravelmente o tempo que um serviço de rede fica indisponível para o usuário final, criando um ambiente proativo na resolução de problemas dos serviços dos ativos que compunham a sua rede de computadores.

Em Fernandes (2013), é apresentado a utilização da ferramenta de monitoramento Zabbix na resolução proativa de problemas de indisponibilidade de enlaces, nas unidades da FAB (Força Aérea Brasileira). Ele também identificou falhas não detectadas (em tempo hábil) de disponibilidade, desempenho e integridade dos serviços de servidores interligados à rede da instituição. Falhas estas, que comprometem severamente a qualidade dos serviços prestados pelas unidades dessa organização em suas atribuições legais perante a federação. Com a implantação da ferramenta de monitoramento Zabbix e com o alinhamento da resolução dos problemas de redes da FAB, baseados nos princípios da governança de Tecnologia da Informação, o cenário da saúde dos serviços de redes obteve uma melhora significativa na sua disponibilidade e manutenção destes serviços.

Filho (2010) diz: “visando alcançar um diagnóstico mais preciso da infra-estrutura da rede, escolhemos uma ferramenta de monitoramento de rede de nome Zabbix, que se apresentou como uma das soluções mais completas disponíveis do mercado”. Nesse artigo, o autor mostra como é importante a escolha de uma ferramenta de monitoramento, que esteja ligada aos problemas que são apresentados no âmbito ao qual está direcionado o ambiente a ser monitorado. Na análise feita durante o trabalho proposto em Filho (2010), evidencia-se que o Zabbix se mostrou muito robusto e adaptável aos mais diferentes cenários de monitoramento. Com sua aplicabilidade de fácil implementação, é um fator atraente para utilização dessa ferramenta como uma solução viável e confiável para monitorar os mais diversos serviços, servidores e ativos conectados à rede.

No trabalho mostrado em Oliveira et al. (2013) a autora propõe monitorar o desempenho e a disponibilidade das máquinas na nuvem privada. Com dois conjuntos de métricas: um para o monitoramento das máquinas físicas e o outro para as máquinas virtuais. Depois de alguns ajustes e problemas na implantação do cenário proposto no trabalho, foi percebida a capacidade do Zabbix de modo satisfatório, de monitorar aspectos importantes para manter a boa funcionalidade da nuvem privada e sua disponibilidade.

O trabalho proposto em Bonomo (2006) fez uma análise de uma ferramenta que atua nas áreas da “Gerência de Rede”, auxiliando o administrador a obter mais informações necessárias para manter o bom funcionamento da rede, minimizando o problema de falta de controle em um ambiente computacional. A ferramenta escolhida para ser usada como auxílio ao administrador foi o Zabbix, pois disponibiliza inúmeros recursos na ajuda da administração de rede. Como gráficos de maior desempenho na coleta dos dados em tempo real e com mais informações, alertas de erros ocorridos nas entidades gerenciadas, configurações, auditoria dos dados etc. Então, foi demonstrado com esse trabalho, a implantação e configuração de uma poderosa ferramenta usada para o gerenciamento e monitoração de redes de computadores.

CAPÍTULO 3 - FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são explanados, tópicos que nortearam a elaboração do presente trabalho. Desde a descrição sobre as áreas funcionais do gerenciamento e seus níveis de atuação, passando a descrever o protocolo de gerenciamento SNMP (*Simple Network Management Protocol*), e a base de informações MIB (*Management Information Base*).

3.1 Áreas Funcionais do Gerenciamento

O modelo OSI (*Open Systems Interconnect*) estabelece 5 áreas de gerenciamento (ver Figura 1). Segundo Eler (2015), “a função destas áreas funcionais é definir o que deve ser monitorado em uma rede e qual a profundidade do gerenciamento a ser executado em cada área”. As áreas funcionais do gerenciamento são as seguintes (ELER, 2015):

- Gerenciamento de Falhas: deve monitorar os estados dos recursos, analisando em que ponto da rede e em que momento, uma falha ou um erro podem ser ocasionados. Uma falha é algo que necessita uma intervenção imediata na resolução. Por exemplo, uma queda em um enlace de comunicação. Já um erro, é algo ocasional que pode ser corrigido ou compensado. Por exemplo, um erro de bits ou falha de sincronismo em um enlace de comunicação. O gerenciamento de falhas atua no isolamento do ponto de falha, bem como na implantação de alternativas até que se chegue à solução definitiva do problema, a fim de minimizar o impacto causado pela parada do sistema como um todo, e por fim, consertar a falha retornando à situação inicial;
- Gerenciamento de Contabilidade: com a função de aferir e verificar os limites de uso dos recursos da rede, aplicando divisão de cotas por usuários ou grupos de usuários, pode inclusive aplicar cobrança diferenciada por tráfego e utilização de recursos da rede;
- Gerenciamento de Configuração: Uma rede de computadores deve estar constantemente em evolução, ou seja, equipamentos são retirados ou acrescentados à rede a todo momento. O gerenciamento de configuração faz com que seja possível atualizar os dados de *hardware* e *software* pertencentes à uma

rede, contando com informações de configurações de todos os ativos. Isso permite, por exemplo, que se reduza o tempo exigido para troca de equipamentos defeituosos em caso de existência de um *backup* das configurações desse ativo;

- Gerenciamento de Desempenho: é a partir dele que se torna possível planejar ações no futuro em uma rede de computadores, pleitear resoluções para problemas rotineiros de fornecedores, além de garantir o cumprimento de SLA, criação de relatórios de desempenho da rede, para fins de demonstração do impacto causado pelas interrupções no negócio da organização etc. A meta aqui é quantificar, medir, informar, analisar e controlar o desempenho dos diferentes ativos da rede;
- Gerenciamento de Segurança: onde se preza pelo resguardo dos ativos da rede, monitorando e identificando violações da política de segurança definida. Desta forma, o gerenciamento de segurança tem como meta supervisionar o acesso aos equipamentos da rede.

Figura 1 - Área de Gerenciamento

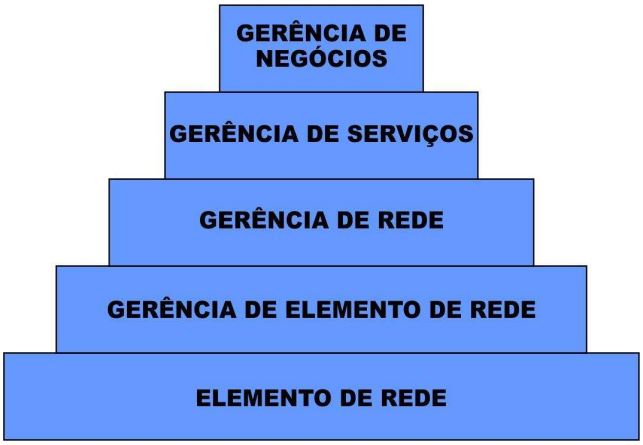
Fonte: (ELER, 2015, p. 4)

Importante se faz tomar conhecimento dos níveis de gerenciamento a que uma solução de gerenciamento tem a capacidade de atingir. Os níveis de gerenciamento (ver Figura 2) definem como a integração do gerenciamento da rede será realizada (ELER, 2015).

Ainda de acordo com Eler (2015), “cada nível possui um conjunto de requisitos de gerenciamento que determinam o nível de gerenciamento desejado para a rede. O gerenciamento implantado em uma rede pode atuar em todos os níveis ou em alguns apenas”. Estes níveis são detalhados abaixo e foram mostrados em (ELER, 2015):

- Elemento de Rede: situada na base da pirâmide de gerenciamento, diz respeito aos ativos da rede de computadores ou telecomunicações que precisam ser gerenciados, e que tenham funções de gerenciamento. Ex. Roteadores, *Switches*, servidores etc.;
- Gerência de Elemento de Rede: aqui pode se realizar o gerenciamento dos ativos da rede elencados no nível anterior de uma forma mais individualizada. Ex. configuração de dispositivos, verificação de falhas individuais etc.;
- Gerência de Rede: neste nível, as ferramentas de gerenciamento fazem o monitoramento dos ativos da rede e as interligações entre estes ativos;
- Gerência de Serviços: formada por sistemas que se destinam à operação, administração e manutenção de serviços, tais como cadastro de usuários, relacionamento com usuários, fornecimento e manutenção de serviços, informações de faturamento, dentre outros. Através do gerenciamento no nível de serviço é praticável, por exemplo, garantir que um SLA está sendo cumprido;
- Gerência de Negócio: aborda os pontos referentes às finanças, aos interesses dos acionistas, dos clientes, dos empregados e da sociedade, ou seja, aborda a visão estratégica da organização e o relacionamento com a área de informática. Grande parte das organizações veem a área de informática ou de Telecomunicações como sendo gastos desnecessários, por isso é necessário demonstrar a relevância destas áreas para os negócios da empresa. Porém, poucas soluções de gerenciamento executam o gerenciamento neste nível mais elevado.

Figura 2 - Níveis de Gerenciamento



Fonte: (ELER, 2015, p. 4)

3.2 Protocolos de Gerenciamento

A seguir, são descritos os protocolos de gerenciamento SNMP (*Simple Network Management*) e MIB (*Management Information Base*), necessários para o monitoramento de dispositivos de rede, como *switches,* roteadores etc.

3.2.1 SNMP (Simple Network Management Protocol)

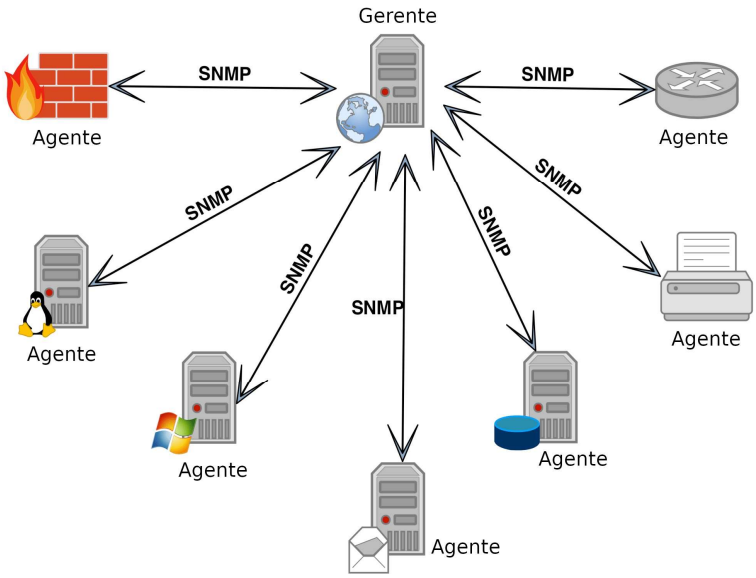
Segundo Mauro e Schmidt (2001), “o núcleo do SNMP é um conjunto simples de operações (e das informações obtidas por essas operações) que permitem ao administrador modificar o estado de alguns dispositivos que suportam agentes SNMP”. Ele é o protocolo padrão para gerência de redes IP, definido através da RFC 1157 (CASE et al., 1990), sendo flexível e de fácil implementação, ele pertence à camada de aplicação da arquitetura OSI (*Open System Interconnection*), fazendo-se valer da camada de transporte e seus serviços do protocolo UDP (*User Datagram Protocol*) para enviar e receber suas mensagens de requisições através da rede (DIAS E ALVES JR., 2002).

O funcionamento do SNMP é baseado em dois dispositivos: o agente e o gerente, os quais trocam mensagens de requisição entre si, no estilo cliente-servidor, conforme é ilustrado na Figura 3. De acordo com Dias e Alves Jr. (2002):

> Cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual. Estas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

Sua simplicidade está no fato dos comandos serem limitados e baseados no mecanismo de busca/alteração, onde é possível realizar operações de alteração de valor de um objeto, de requisição de seu valor e suas variações. Além disso, o fato de utilizar esse pequeno número de operações, gera como consequência, a redução do tráfego de mensagens de gerenciamento através da rede, o que permite a implementação de novas características (DIAS E ALVES JR., 2002).

Figura 3 - O gerente e os agentes SNMP



Fonte: (MACÊDO, 2017)

3.2.1.1 O Agente SNMP

O Agente SNMP é a peça de *software* executada nos dispositivos da rede que estão sendo gerenciados. Pode ser um programa separado ou pode ser incorporado ao sistema operacional, por exemplo, o *IOS* da Cisco em um roteador, ou o sistema operacional de baixo nível que controla um nobreak (MAURO E SCHMIDT, 2001). O agente tem a função de coletar dados sobre o equipamento gerenciado e armazená-los em uma base de dados local, conhecida como MIB (*Management Information Base*). Quando o gerente requisita uma determinada informação sobre o equipamento gerenciado, o agente coleta essa informação no respectivo elemento e a envia ao gerente (ZARPELÃO, 2012).

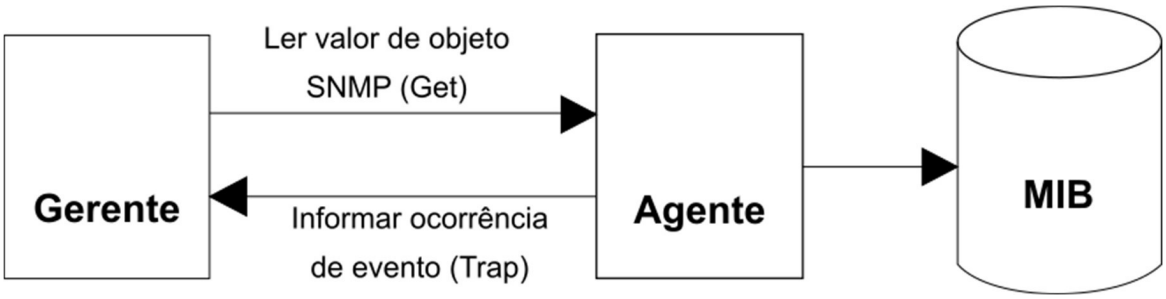
Segundo Mauro e Schmidt (2001), o agente também se encarrega de notificar o gerente caso ocorra alguma exceção no dispositivo gerenciado. Tais dispositivos podem manifestar falhas ou comportamentos inadequados e ao identificar a ocorrência de tal evento, o agente endereça pacotes informativos, relatando o fato às estações de gerência cadastradas em sua lista de distribuição de alarmes. Essa operação é realizada através de interrupções (*traps*), que podem ou não informar com detalhe o que ocorreu de forma inesperada no dispositivo. Há ainda a possibilidade de a estação de gerenciamento realizar consultas para investigar e obter mais detalhes sobre o ocorrido.

3.2.1.2 O Gerente SNMP

Ainda segundo Mauro e Schmidt (2001), "um gerente é um servidor executando algum tipo de sistema, que pode lidar com tarefas de gerenciamento de uma rede". É possível que se adote um ou mais gerentes em execução em uma mesma estação, que colaboram mutuamente na realização do gerenciamento, com todos utilizando o protocolo de gerência proveniente dessa estação. O gerente envia comandos aos agentes para solicitar as informações das variáveis de um objeto gerenciado ou para modificar o valor de uma determinada variável. Os gerentes então tratam as informações extraídas pelos agentes e as retornam à aplicação que originalmente as requisitou.

A Figura 4 mostra que a comunicação entre o agente e gerente, se dá através de operações e notificações adotadas pelo protocolo SNMP. Depois de coletadas, as informações sobre objetos são armazenadas nas MIB´s, que são implantadas juntamente com os agentes nos elementos gerenciados. Os agentes então, guardam as informações sobre o funcionamento dos dispositivos e dos processos que executam os protocolos de comunicação (PINHEIRO, 2011).

Figura 4 - A troca de informações entre o gerente e o agente SNMP e seu armazenamento na MIB



Fonte: (Adaptado de PINHEIRO, 2011)

Quando o *software* de gerência é iniciado, ele não possui nenhuma informação sobre a configuração ou funcionamento da rede. Tais informações vão sendo coletadas através das respostas que são remetidas pelos agentes. A partir daí, o gerente realiza *polling* (consultas periódicas) para manter a comunicação com os agentes, tornando possível o mapeamento, monitoração e controle da rede por parte do *software* de gerência (PINHEIRO, 2011).

3.2.1.3 SNMP v1

SNMPv1 é a primeira versão do SNMP. É fácil de configurar, pois requer apenas uma comunidade de texto simples (ABREU E PIRES, 2014).

Embora tenha desempenhado suas funções de maneira satisfatória, essa versão deixava a desejar principalmente em questões de segurança.

Abreu e Pires (2014) consideram fraca a segurança desta versão; as senhas são baseadas em *community strings*, que são simples e em formato texto aberto, que permitem que qualquer ferramenta de gerência que conheça esta *string* obtenha acesso aos dados deste dispositivo.

3.2.1.4 SNMP v2

O SNMPv2 acarreta algumas vantagens, como melhorias na eficiência e no desempenho (PINHEIRO, 2011).

Segundo Stallings (1999), as operações *Get*, *GetNext* e *Set* usadas no SNMPv1 são idênticas às usadas no SNMPv2. No entanto, a principal vantagem do SNMPv2 sobre as versões anteriores é o comando *Inform*. Ao contrário dos *Traps*, que são simplesmente recebidos por um gerente, os *Informs* são confirmados positivamente com uma mensagem de resposta. Se um gerente não responder a um *Inform*, o agente SNMP enviará o *Inform* (PINHEIRO, 2011).

3.2.1.5 SNMP v3

De acordo com Mauro e Schmidt (2001), a única alteração relevante da terceira versão do protocolo SNMP (SNMPv3) trata os problemas de segurança que se manifestaram nas versões anteriores (SNMPv1 e SNMPv2).

Segundo Pinheiro (2011), SNMPv3 é a versão mais recente do SNMP. Seus recursos de estrutura de gerenciamento envolvem principalmente segurança aprimorada. A arquitetura SNMPv3 apresenta o modelo de segurança com base no usuário (USM) para segurança de mensagens e o modelo de controle de acesso baseado em visualização (VACM) para controle de acesso.

3.3 MIB (Management Information Base)

De acordo com Dias e Alves Jr. (2002), MIB é a base de informações de gerenciamento, onde são armazenadas as informações dos objetos gerenciados. Para que um gerente SNMP, por exemplo, saiba que informações podem ser solicitadas a um agente, como também que informações de alerta (*traps*) poderão ser enviadas do agente para o gerente.

O RFC 1066 (MCCLOGHRIE E ROSE, 1988) definiu a primeira versão da MIB. Este padrão expôs e estabeleceu o que é necessário para o monitoramento e o controle de redes baseadas nos protocolos TCP/IP. Sua atualização ocorreu com o RFC 1213 (MCCLOGHRIE E ROSE, 1991), que apresentou uma segunda MIB, a MIB II. Basicamente são definidos três tipos de MIB´s: MIB II, MIB experimental, MIB privada (GUILLERMO, 2008).

A MIB II, que é tida como uma evolução da MIB I, tornando-a obsoleta, provê dados gerais de gerenciamento de um equipamento específico. Através da MIB II é possível obter dados como: número de pacotes transmitidos, estado da interface, entre outras (GUILLERMO, 2008).

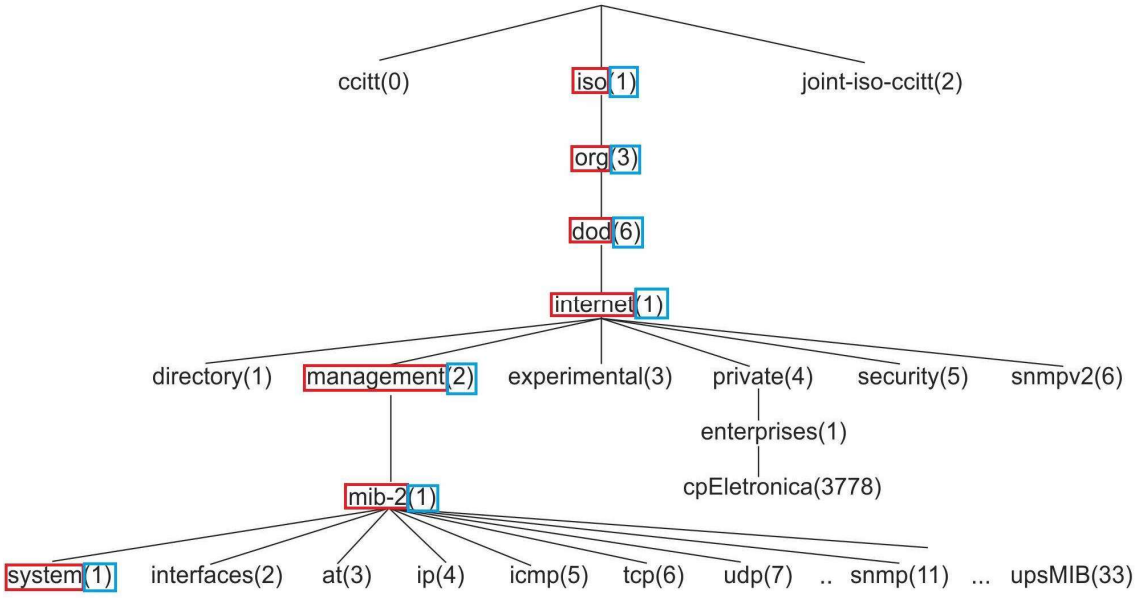
A MIB experimental é um estágio que tem seus componentes (objetos) em fase de desenvolvimento e teste. De forma geral, elas proveem características mais particulares a respeito da tecnologia dos meios de transmissão e equipamentos utilizados (GUILLERMO, 2008).

MIB privada é aquela que tem seus componentes fornecendo informações detalhadas sobre os dispositivos gerenciados, como configuração e colisões. Também é possível reinicializar, desabilitar uma ou mais portas de um roteador (GUILLERMO, 2008).

Composta de uma estrutura em árvore (ver Figura 5), que contém variáveis de gerência de determinado equipamento, a MIB estabelece para cada variável um identificador único chamado OID (*Object Identifier*). Em suma, os objetos estabelecidos nos padrões oficiais podem ser exclusivamente identificados. Para encontrar determinada informação, o identificador da variável que será requisitada por um gerente SNMP, por exemplo, é composto pelo IP do equipamento juntamente com o identificador do objeto na árvore MIB (OID) (CONTESSA E POLINA, [20-]).

Os objetos da árvore que não são folhas ligam outros objetos relacionados, que estampam os dados tratados nos agentes SNMP (ou elementos gerenciados). Dessa forma, podemos dizer que uma variável MIB seria a instância de um objeto da árvore, e que essa instância é o que pode ser de fato manipulada pelo protocolo SNMP (CONTESSA E POLINA, [20-]).

Figura 5 - Árvore MIB parcial a partir da raiz



Fonte: (CONTESSA E POLINA, [20-], p. 4)

Um objeto é localizado através do caminho percorrido da raiz até o objeto desejado. Como exemplo, temos um objeto com o *Object Identifier* (OID) correspondente ao caminho iso.org.dod.internet.mgmt.mib-2.system.sysDescr (em vermelho na Figura 5). Ele identifica um objeto simples, que tem somente uma única instância, a qual é dado o nome simbólico de iso.org.dod.internet.mgmt.mib-2.system.sysDescr.

O nome numérico que equivale a esse nome simbólico seria 1.3.6.1.2.1.1.1.0 (em azul na Figura 5). Comparando o nome numérico e o nome simbólico, vemos que ambos percorrem o mesmo caminho na árvore.

CAPÍTULO 4 - PLATAFORMAS DE GERENCIAMENTO

Neste capítulo são apresentadas algumas características de funcionamento das plataformas de gerenciamento Nagios, Dude além das plataformas adotadas, que são Zabbix e Grafana, ilustrando como estas plataformas reúnem as melhores características em relação às duas primeiras.

4.1 Nagios

Segundo Henrique (2014), Nagios é uma ferramenta de monitoramento de rede que fornece todos os recursos em um único pacote. O Nagios monitora os servidores e os dispositivos de rede e avisa quando um determinado serviço que está sendo monitorado está em falha, além de avisar quando o serviço volta ao estado requerido normal. Nagios é capaz de executar as seguintes atividades (HENRIQUE, 2014):

- O monitoramento de diferentes serviços em um servidor, como SMTP, HTTP, POP, IMAP, PROXY;
- Monitoramento constante dos recursos do servidor, como processador, memória etc.;
- Uma *interface web* agradável que indica o status dos serviços por três métodos: OK, Aviso, Crítico;
- Mantém um conjunto diferente de grupos de contatos (que conterão endereços de e-mail de diferentes pessoas interessadas), com base no serviço.

4.2 Dude

O Dude é um *software* de gerenciamento de redes de computadores gratuito que oferece monitoramento de rede, mapeamento de rede além de outras características (LASKOSKI, [20-]).

Este *software* pode ajudar os administradores de rede a concluir determinadas tarefas: desde tarefas básicas de monitoramento, como garantir a disponibilidade dos computadores ou servidores, até operações mais sofisticadas, como monitoramento de enlaces ou gerenciamento de dispositivos (LASKOSKI, [20-]).

Segundo Laskoski ([20-]), o monitor de rede do Dude é um aplicativo da Mikrotik, que pode melhorar drasticamente a maneira como se gerencia um ambiente de rede. Ele varre automaticamente todos os dispositivos dentro de sub-redes especificadas, desenha e faz o layout de um mapa de suas redes, monitora os serviços de seus dispositivos e o alerta caso algum serviço tenha problemas (LASKOSKI, [20-]).

4.2.1 Recursos do DUDE

Laskoski ([20-]) detalha os seguintes recursos proporcionados pelo DUDE:

- Descoberta e *layout* automáticos da rede;
- Faz descoberta das configurações de *hardware* dos dispositivos;
- Suporta monitoramento SNMP, ICMP e DNS;
- Define notificações sonoras baseados em *triggers* para os dispositivos monitorados;
- Facilidade de instalação e utilização;
- Permite desenhar seus próprios mapas e adicionar dispositivos personalizados;
- Monitoramento e gráficos de desempenho de enlaces individuais;
- Acesso direto às ferramentas de controle remoto para gerenciamento de dispositivos;
- Suporta servidor Dude remoto e cliente local.

4.3 Zabbix

O Zabbix “é uma ferramenta moderna, *open source* e multiplataforma, com sistema de monitoramento distribuído, capaz de monitorar a disponibilidade e o desempenho da infraestrutura de uma rede, além de aplicações” (HORST et al., 2015).

Segundo Zabbix Sia (2018), o Zabbix é uma solução *open source* de monitoração para empresas, ou seja, desenvolvido e distribuído de acordo com a GPL (*General Public License* versão 2). Isso assegura que seu código-fonte é distribuído gratuitamente e está disponível para o público em geral. Porém, há também o suporte comercial, fornecido pela Zabbix SIA.

Ainda segundo Zabbix Sia (2018), o Zabbix é capaz de monitorar vários parâmetros de um ambiente de rede de computadores, além da saúde e integridade de

servidores. O Zabbix faz uso de um mecanismo de notificação flexível que permite aos administradores, configurarem alertas de *e-mail* baseados em praticamente qualquer evento. Isso proporciona uma rápida reação da equipe de informática para a resolução de problemas em servidores críticos ao negócio da empresa. O *software* oferece ainda, relatórios e visualização de dados com riqueza de características com base nos dados coletados e armazenados em banco de dados. Isso torna o Zabbix, ideal para o planejamento de capacidade.

Zabbix Sia (2018) explica que o Zabbix suporta *polling* e *trapping*, citados anteriormente. Todos os relatórios do Zabbix e suas estatísticas, bem como seus parâmetros de configuração, são obtidos por meio de ferramenta *web*, definida como o *front-end* do produto. A ferramenta *web* garante que o status da rede e da saúde dos servidores possa ser checada a partir de qualquer lugar no mundo e em qualquer dispositivo com acesso à *Internet*. Configurado corretamente, o Zabbix contribui de maneira importante no controle da infraestrutura de Tecnologia da Informação, tanto para pequenas empresas, com poucos servidores, quanto para grandes empresas, com muitos ativos de rede (ZABBIX SIA, 2018).

4.3.1 Funcionalidades

Segundo Horst et al. (2015), o Zabbix conta com vários módulos e algumas de suas funcionalidades são:

- Descoberta automática de dispositivos de rede e recursos do *host*;
- Monitoramento distribuído por meio do uso de *proxy*;
- Aplicação servidor compatível com diferentes sistemas operacionais;
- Monitoramento com ou sem o uso de agentes;
- Suporte a todas as versões do SNMP;
- Tradução para vários idiomas;
- Autenticação segura de usuário;
- Permissões flexíveis;
- Monitoramento de aplicações Java;
- Monitoramento de dispositivos via IPMI (Intelligent Platform Management Interface);
- Envio de alertas por e-*mail*, SMS, Jabber, XMPP e scripts personalizados;

- Monitoramento de aplicações *web*;
- Monitoramento de ambientes virtualizados.
- Agentes disponíveis para diversas plataformas;
- Suporte total ao IPv6;
- Integração com diferentes tipos de banco de dados.

4.3.2 Módulos

O Zabbix é composto de vários módulos, são eles: o Zabbix Server, o Zabbix Agent, o Zabbix Proxy, o Java Gateway, a Interface Web e o Banco de Dados (HORST et al., 2015).

O módulo Zabbix Server é o cérebro do sistema, com a capacidade de monitorar remotamente os serviços de rede (*web* e *e-mail*) utilizando checagens simples (HORST et al., 2015). É o componente central para onde os agentes enviam as informações e estatísticas coletadas sobre disponibilidade e integridade dos equipamentos monitorados. O módulo recebe as coletas, as processa, produz relatórios, envia alertas além de realizar comandos para casos pré-configurados (HORST et al., 2015).

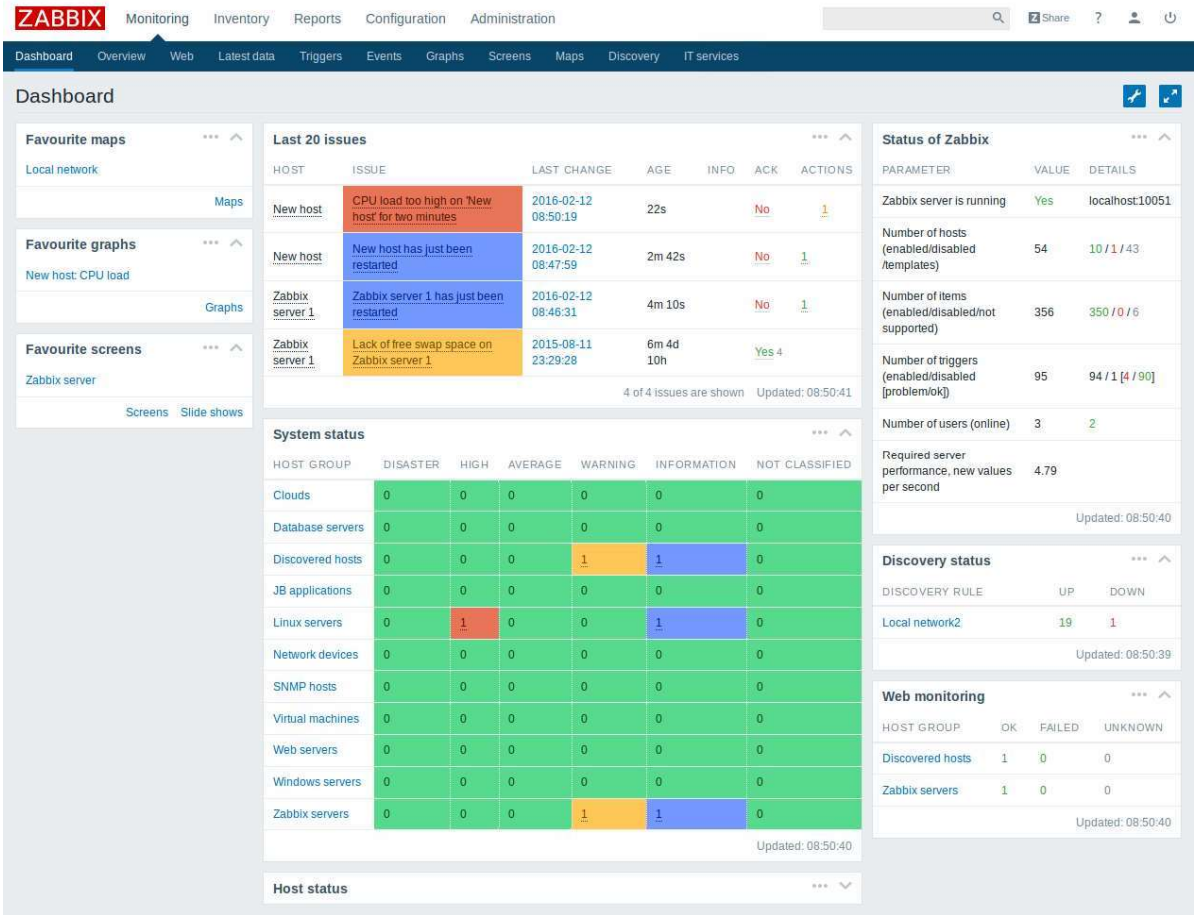
Segundo Lima (2014), o módulo Zabbix Agent é responsável por coletar as informações dos ativos de rede gerenciados e enviá-las ao Zabbix Server ou Zabbix Proxy. Ele envia através do protocolo de JSON na porta 10050/10051 do servidor, as respostas das requisições de verificação passiva de dados que são enviadas do servidor ao agente. Além disso, ele também pode monitorar ativamente o uso dos recursos e aplicações por parte dos *hosts* gerenciados, tais como: processos, serviços, aplicativos em execução, disco rígido etc.

Ainda de acordo com Lima (2014), o módulo Zabbix Proxy é semelhante ao Zabbix Server, funcionando basicamente em nome dele (na visão do agente monitorado, o *Proxy* passa a ser o Zabbix Server), coletando informações de desempenho e disponibilidade dos ativos de rede gerenciados. Todos os dados recebidos são armazenados temporariamente, transferidos ao Zabbix Server a que o Zabbix Proxy pertencer. A utilização deste componente é opcional, mas normalmente é muito benéfica, pois, como visto, distribui a carga de monitoração normalmente atribuída ao Zabbix Server, devido à sua capacidade de coletar milhares de informações por segundo e armazená-las em seu banco de dados.

Lima (2014) define que a *Interface Web* (*Frontend*), é o módulo onde o administrador de rede propriamente interage com os dados do Zabbix Server, permitindo a personalização das configurações de seu monitoramento. É nele onde os usuários do Zabbix acessam mapas, gráficos e telas de acordo com regras de controle de acesso (LIMA, 2014).

A Figura 6 mostra a tela inicial do Zabbix, que pode ser acessada através da sequência de menus MONITORAMENTO > DASHBOARD. Nela, tem-se um resumo dos avisos emitidos pelo sistema onde, após prévia configuração, os *tickets* em verde, mostram os componentes em funcionamento normal; em azul indicam apenas informações, como mudança de estado; laranja claro indicam pontos que merecem atenção, antes que algo mais sério aconteça; laranja escuro indica problema de severidade alta, e que algo deve ser feito para corrigir o problema o quanto antes; e vermelho indica problema crítico, algo deve ser feito imediatamente, fatalmente o serviço ou servidor já pode estar parado (LIMA, 2014).

Figura 6 - Tela principal do Zabbix, o *dashboard*

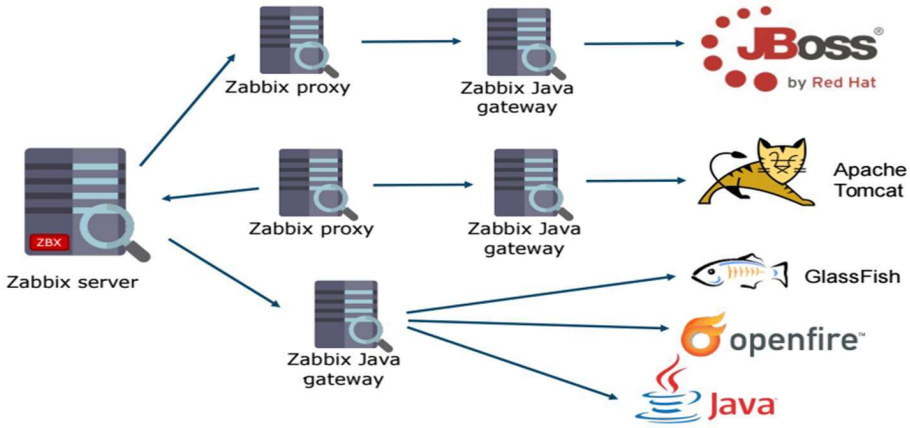


Fonte: (ZABBIX SIA, 2018)

O Banco de Dados (BD) é o módulo encarregado de armazenar as informações coletadas pelo Zabbix Server ou Zabbix Proxy, além das configurações do sistema (LIMA, 2014). O BD pode ser acessado tanto pelo Zabbix Server através da linha de comando do terminal, quanto pela *Interface Web* do Zabbix.

Segundo Lima (2014), o Zabbix Java Gateway é um processo de *background* (*daemon*) escrito em Java, e a partir da versão 2.0, foi implementado como suporte nativo ao monitoramento das aplicações JMX (*Java Management Extension*). Quando o Zabbix Server precisa coletar um item (dado) através de um contador JMX em um *host*, ele solicita ao Java Gateway, que utiliza a API de gerência JMX para requisitar da aplicação o dado de interesse. O Java Gateway aceita conexões advindas do Zabbix Server e do Zabbix Proxy e só pode ser utilizado como um "proxy passivo". Ao contrário do que ocorre com um Zabbix Proxy, o Java Gateway pode estar atrás de outro *proxy* (um Zabbix Proxy), como ilustrado na Figura 7.

Figura 7 - Exemplos de aplicação do Zabbix Java Gateway



Fonte: (ZABBIX SIA, 2018)

4.4 Grafana

O monitoramento de redes está hoje em perceptível crescimento e cada vez mais popular em empresas que passam a dedicar seus esforços nessa direção. O Zabbix como carro chefe neste ramo, tem dado um grande suporte aos administradores de redes em suas tarefas nesse sentido, além dos inúmeros benefícios proporcionados por ele de forma nativa, não são poucos os que ainda buscam um "algo a mais" para apresentar interfaces mais bonitas, simplistas e mais interativas (SALITURO, 2020).

Com a API do Zabbix é possível desenvolver diversas atividades desde consultas, execução de tarefas e integrações entre sistemas. Na Zabbix Conference de 2015 foi apresentada, em forma de estudo de caso, uma ferramenta que se integrava ao Zabbix: o Grafana (ZOBNIN, 2015). Ele é uma ferramenta que permite mostrar vários dados coletados de outras ferramentas em uma interface mais visualmente atrativa. Ele tem se revelado uma excelente solução para painéis visuais mais elegantes e intuitivos aos olhos dos usuários.

Segundo Salituro (2020), o Grafana tem um futuro promissor, pois é uma ferramenta que possibilita um grande auxílio na visualização dos dados, devido à sua capacidade de encantar superiores de diversas áreas de atuação através de seus gráficos. Além de ser uma ótima solução gratuita e de código aberto, sua estrutura leve e *multi data source* proporciona versatilidade no seu uso, pois possui integração com diversas soluções além do Zabbix, como o MySQL[1], GLPI[2], PostgreSQL[3], Google Agenda[4], InfluxDB[5] entre outras. Assim, é possível montar painel visual com diferentes dados provenientes de diferentes fontes de coleta. Um exemplo disso seria um único painel de monitoramento de um centro de suporte, contando com informações das principais métricas do atendimento via telefone, *chat*, ferramenta de chamados e ferramenta de monitoramento.

Outra enorme vantagem do Grafana é que, por ser *open source*, a comunidade participa bastante no seu desenvolvimento, documentando muito do progresso alcançado, além de ter o fórum bem ativo junto a milhares de usuários em todo o mundo. Assim, não é difícil encontrar ajuda ao se deparar com um problema em sua implantação, operação e manutenção (SALITURO, 2020).

A Figura 8 ilustra um painel visual que exibe diversos parâmetros monitorados de um Servidor Zabbix, como uso de processador, espaço livre em disco etc. Já a Figura 9, mostra um dado de um item em forma de gráfico que exibe especificamente o uso de memória de um dispositivo monitorado.

---

[1] Sistema de gerenciamento de banco de dados, que utiliza a linguagem SQL como *interface*. Site oficial: https://www.mysql.com

[2] Sistema de código aberto para Gerenciamento de Ativos de TI, rastreamento de problemas e central de serviços. Site oficial: https://glpi-project.org/pt-br

[3] Sistema gerenciador de banco de dados objeto relacional, desenvolvido como projeto de código aberto. Site oficial: https://www.postgresql.org

[4] Serviço de agenda e calendário *on-line* oferecido gratuitamente pela empresa Google. Site oficial: https://www.google.com

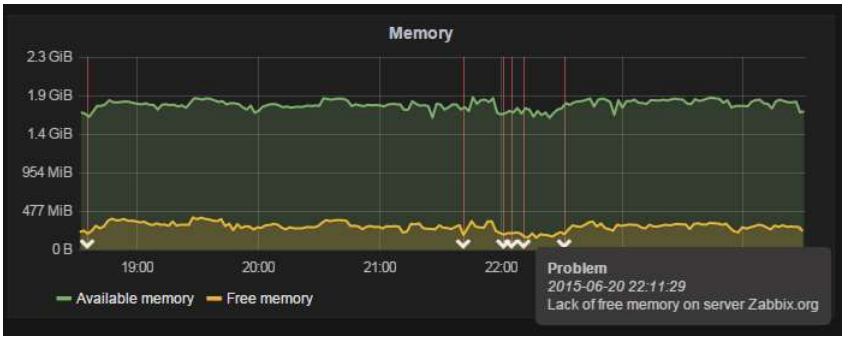
[5] Banco de Dados de séries temporais de código aberto desenvolvido pela InfluxData. Site oficial: https://www.influxdata.com

A integração com as ferramentas citadas é feita por meio de plugins e em particular, com o Zabbix, o plugin foi proposto em (ZOBNIN, 2015).

Figura 8 - Exemplo de painel visual do Grafana

Fonte: (PIRES, 2019)

Figura 9 - Exemplo de gráfico do Grafana



Fonte: (PIRES, 2019)

4.4.1 Funcionalidades

Segundo Salituro (2020), o Grafana possui diversas funcionalidades, tais como:

- Filtros. Consultas provenientes de diversas fontes de dados como o Zabbix Server, MySQL, GLPI etc.;

- Alertas automáticos com base em *triggers*. Permite anexar regras aos painéis de controle. Quando um painel é salvo, o Grafana extrai as regras de alerta em um armazenamento separado de regras de alerta e as programa para avaliação;

- Variáveis. Permitem que se crie painéis que possam ser reutilizados para muitos casos de uso diferentes;

- *Links* entre painéis visuais ou URL externa;

- Criação de grupos de usuários. No caso de empresas que têm um Grafana e várias equipes, é possível que se deseje manter certos dados separados, e compartilhar apenas determinados painéis entre as equipes. Assim, é possível criar grupos de usuários, definindo permissões especiais em pastas, painéis etc.;

- Anotações. Este recurso, que aparece como um marcador de gráfico no Grafana, é útil para correlacionar dados caso algo dê errado;

- Manipulação de eixos e legendas dos gráficos. Com isso, tornando os painéis mais intuitivos para o entendimento de qualquer pessoa;

- *Playlist*. Uma lista de painéis exibidos em uma sequência. Pode-se usar uma lista de reprodução para criar consciência situacional ou apresentar métricas para equipes ou visitantes;

- Autenticação LDAP. Permite conectar usuários para organizações através do banco de dados de usuários, como o *Active Directory* do *Windows*, dessa forma, fornecendo automaticamente às pessoas, acesso aos painéis designados para suas equipes;

- Exportação e importação em JSON. Os painéis são exportados no formato JSON e contêm tudo o que é necessário (*layout*, variáveis, estilos, fontes de dados, consultas etc.) para que o painel seja importado posteriormente.

CAPÍTULO 5 - METODOLOGIA

No que diz respeito ao conceito de método científico, foram trazidas duas grandes áreas: pesquisa bibliográfica e pesquisa experimental, de modo que ambas sejam capazes de delinear o desenvolvimento deste trabalho.

Com as pesquisas bibliográficas relacionadas à rede de computadores, gerenciamento de rede, protocolo de gerenciamento, Zabbix e Grafana, foi possível assim, construir uma base de conhecimento sobre as ferramentas de monitoramento, cumprindo com o objetivo tema deste trabalho.

Com a pesquisa experimental é possível entender os modos de funcionamento do sistema, e com isso contribuir para a criação de manuais de instalação, realizando a instalação do Zabbix Server em um servidor dedicado, a instalação do Zabbix Agent em todos os servidores da empresa e a habilitação do protocolo SNMP nos ativos de rede a serem monitorados.

Por meio desta pesquisa é possível criar análises quantitativa e qualitativa dos benefícios da implantação do sistema Zabbix.

Por meio da análise quantitativa é definido e analisado o nível de armazenamento nos HD's (discos rígidos) dos servidores, demonstrando assim, a necessidade de aquisição de mais unidades de armazenamento para a operação e para os *backups*.

Com a análise qualitativa, podemos mensurar o quanto diminuiu o tempo de resposta da equipe de informática da empresa à problemas antigos conhecidos e o *downtime* dos equipamentos, serviços e sistemas.

CAPÍTULO 6 - IMPLANTAÇÃO DO ZABBIX E GRAFANA

O presente estudo visa mostrar a importância do gerenciamento em uma rede corporativa, descrevendo os cenários antes e após a sua implantação na empresa analisada, ilustrando resultados enriquecedores. Implantado o monitoramento para todos os ativos da rede, foram destacados dois pontos importantes para a atividade da empresa: a disponibilidade e espaço em disco dos servidores, destinados ao armazenamento de imagens dos exames e a identificação de melhorias na infraestrutura da rede. Atualmente, a empresa é composta de quatro unidades.

6.1 Infraestrutura de TI

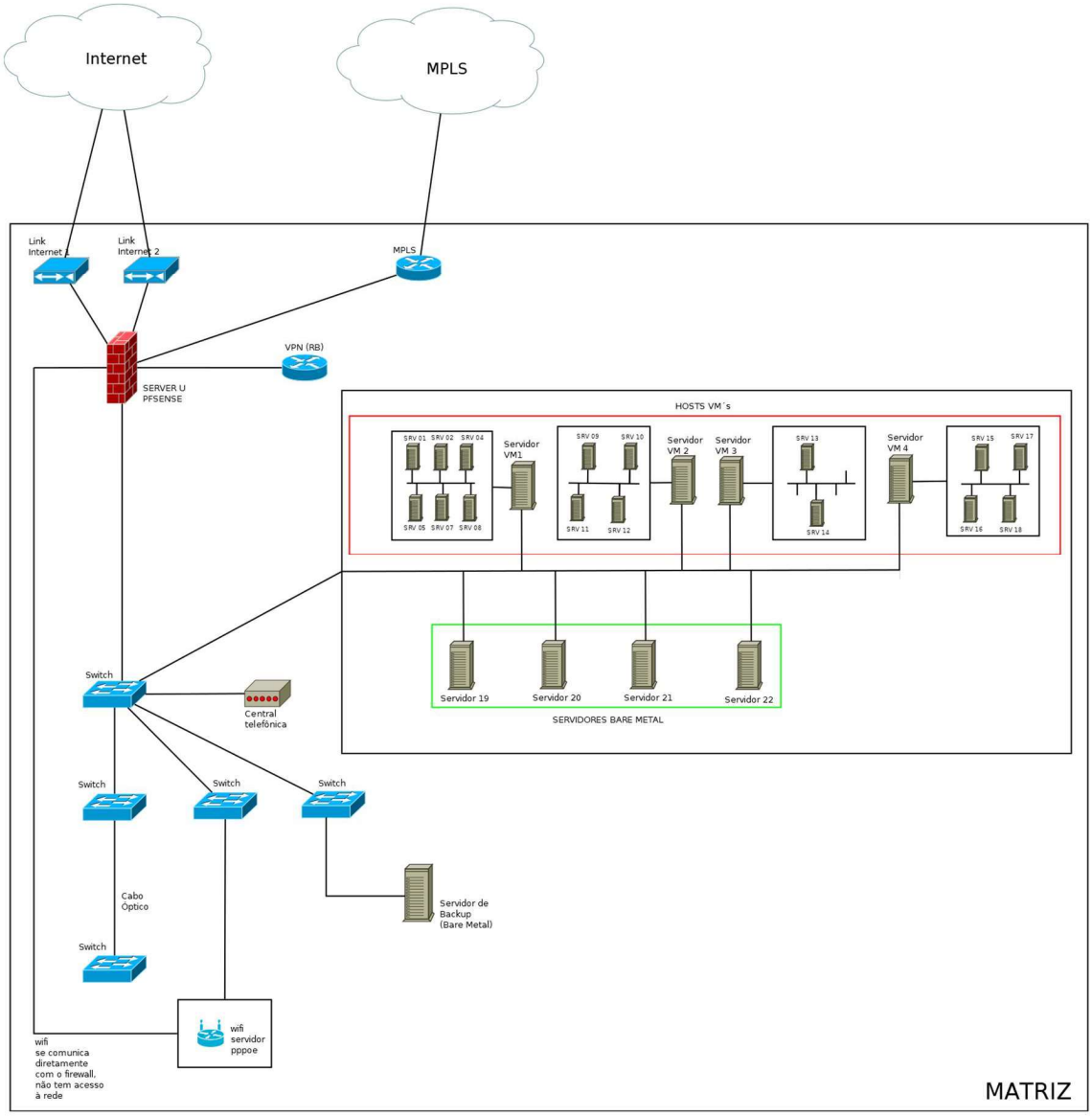
No início de 2018, o cenário da rede era confuso, devido à defasagem de documentação e componentes desatualizados. A empresa contava com muitos serviços terceirizados, inclusive de suporte de informática, administração de *e-mail*, telefonia, câmeras de vigilância, tudo isso sem muito controle. Não era raro haver travamentos de servidores, *switches*, quedas de *Internet* e na rede *MPLS* (PINHEIRO, 2006), sem que esquipe de informática percebesse o problema imediatamente, o que causava muitos transtornos para atender os chamados das 4 unidades.

Em meados de 2018, foi feita a implantação inicial do monitoramento de toda a infraestrutura. Atualmente, ainda em processo de mudança e aperfeiçoamento, as unidades já contam com equipamentos melhores, conforme detalhado a seguir.

6.1.1 Matriz

Esta rede conta com uma topologia mista de estrela e hierárquica, composta de 4 servidores virtuais, suportados pelo *hipervisor VMWARE ESXi* e 5 servidores físicos rodando sob o *Windows Server*; 1 *ServerU* atuando como *firewall*, rodando nele o *PFSense*; 1 roteador *Mikrotik*, fechando uma VPN entre as três filiais e a matriz; 1 central telefônica; 5 *switches* (sendo quatro de 48 portas e um com 24 portas); 5 roteadores *wifi* servindo sinal de *Internet* para clientes; 2 enlaces de *Internet* (sendo um principal e outro como redundância); e um enlace *MPLS* (*Multiprotocol Label Switching*) entre duas das filiais (Figura 10).

Figura 10 - Mapa da infraestrutura de rede da matriz



Fonte: (Autoria Própria)

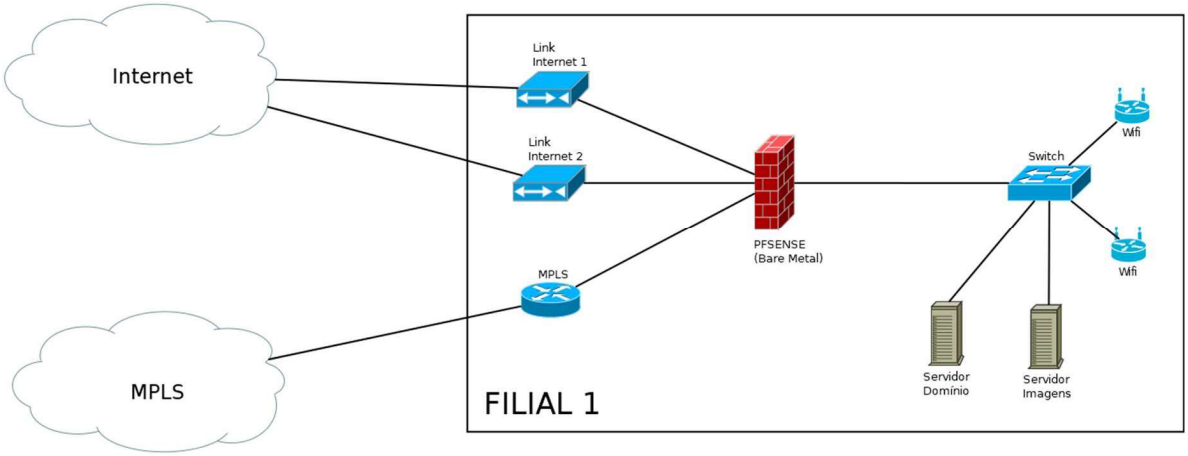
Hoje a rede já conta com uma segmentação do bloco de endereços privados classe A, o que ajuda a configurar um segmento para as estações de trabalho, outro para os servidores, outro para os equipamentos médicos, além de um quarto destinados ao *wifi* para visitantes, proporcionando maior controle de tráfego e segurança da rede.

6.1.2 Filial 1

A filial 1 (ver Figura 11) conta com uma estrutura mais enxuta, sendo 1 PC rodando o *PFSense* atuando como *firewall*; 2 servidores *físicos*; 1 *switch* 48 portas; 2

roteadores *wifi* provendo *Internet* para os clientes; dois enlaces de *Internet* (principal e redundante); e 1 enlace *MPLS* que a interliga com a matriz e a filial 2.

Figura 11 - Mapa da infraestrutura de rede da filial 1

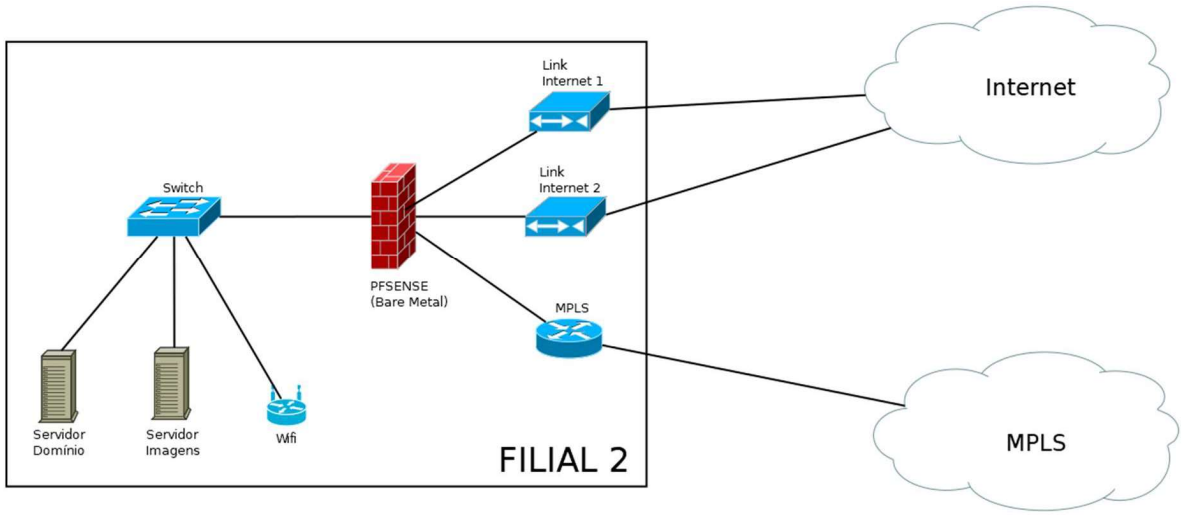


Fonte: (Autoria Própria)

6.1.3 Filial 2

A filial 2, conta basicamente com a mesma estrutura da filial 1 (Figura 12), sendo que, possui apenas 1 roteador *wifi*, localizado na recepção da unidade, uma vez que conta com uma estrutura física mais reduzida em relação a filial 1 e a matriz.

Figura 12 - Mapa da infraestrutura de rede da filial 2

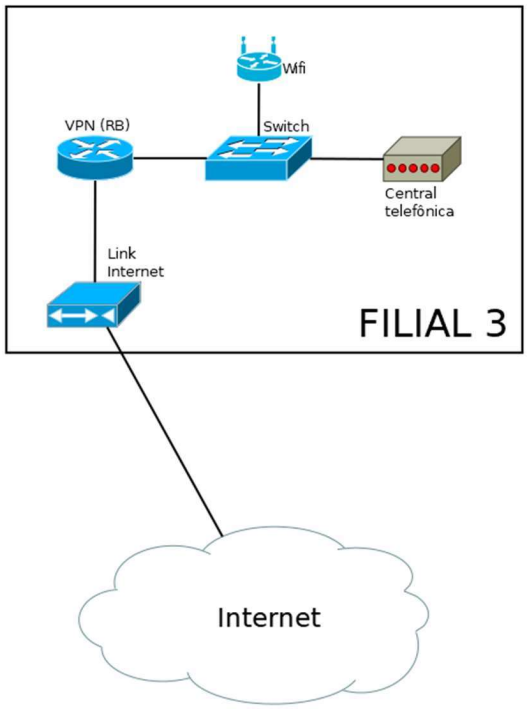


Fonte: (Autoria Própria)

6.1.4 Filial 3

A filial 3, conta com 1 roteador *Mikrotik*, para *VPN* entre ela e a matriz; 1 *switch* 24 portas; 1 central telefônica interligada a central da matriz; 1 enlace de *Internet*; e 1 roteador *wifi* para os clientes (Figura 13).

Figura 13 - Mapa da infraestrutura de rede da filial 3



Fonte: (Autoria Própria)

6.2 Detalhes da Implantação

Para configurar a estrutura de monitoramento do Zabbix, foi estabelecido que, inicialmente seriam monitorados os servidores mais importantes, que são os servidores físicos rodando o *software* de virtualização *VMWare*, por conterem servidores virtuais críticos, como os destinados ao armazenamento de imagem e o do *ERP* da empresa, que eram os que possuíam maior frequência de problemas e reclamações por parte dos colaboradores.

Deles, seriam monitorados a disponibilidade, o uso de memória, uso de processador, uso de HD (quantidade total e espaço livre). Em especial nos servidores de imagens, é monitorado o acesso ao disco (frequência de leitura e escrita), devido ao

seu uso constante, pois a todo momento eles estão recebendo imagens dos exames realizados na empresa.

O ambiente de monitoramento foi montado para rodar sobre servidores virtuais, utilizando as configurações descritas a seguir:

SERVIDOR VIRTUAL 1

- Sistema Operacional: FreeBSD 12.0 64 bits
- Servidor Web Apache 2.4
- PHP 5.6.x
- Zabbix 4.2.x
- Grafana 5.4.x

Para a *interface web* foi instalado o servidor Apache na versão 2.4 e o interpretador PHP na versão 5.6.40. Os pré-requisitos exigidos pelo Zabbix 4.x são 1.3.12 ou superior para o Apache e 5.4.0 ou superior para o PHP. Todos eles e mais o Zabbix Server, o Zabbix Agent e o Grafana foram instalados seguindo a configuração padrão, por meio de compilação de pacotes no FreeBSD em uma instância de servidor virtual.

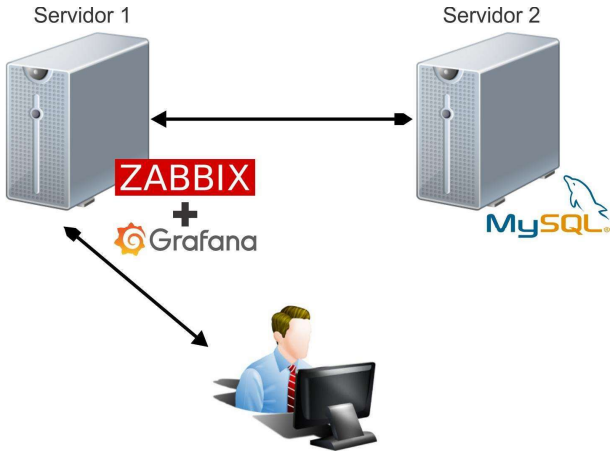
SERVIDOR VIRTUAL 2

- Sistema Operacional: FreeBSD 12.0 64 bits
- MySQL 8.0.x

Para a instalação do Banco de Dados foi escolhido o MySQL em sua última versão à época, por ser popular e um dos recomendados pela instalação do Zabbix. Ele também foi instalado através da compilação de pacotes, sobre o sistema FreeBSD em um servidor virtual separado do Zabbix.

Zabbix, Grafana e MySQL podem ser instalados tanto no mesmo servidor quanto em servidores separados. Buscando um melhor desempenho, evitando assim, um alto processamento em um único servidor virtual, devido a quantidade de acessos ao banco de dados; visando facilitar a recuperação em casos de falhas nos servidores virtuais; e ainda, a previsão de aumento na quantidade de dispositivos monitorados, foi adotado o cenário ilustrado na Figura 14, com o Zabbix e Grafana em um servidor virtual e o MySQL em outro.

Figura 14 - Estruturação dos servidores Zabbix, Grafana e MySQL



Fonte: (Adaptado de PIRES, 2019)

6.2.1 Instalação Zabbix

Primeiro é instalado o servidor Zabbix-Server com os componentes: MySQL, Apache, Net SNMP e Fping que são as dependências necessárias para o cenário que pretendemos monitorar:

```
cd /usr/ports/net-mgmt/zabbix-server
make install clean
```

Em seguida, é criado um banco de dados e um usuário para se utilizar o *backend*:

```
cd /usr/local/share/zabbix/server/create
cat schema/mysql.sql data/data.sql data/images_mysql.sql | mysql -u zabbix -p zabbix

cd /usr/local/etc/zabbix
cp zabbix_server.conf.sample zabbix_server.conf
```

O arquivo zabbix_server.conf - por padrão, é voltado para o monitoramento de redes pequenas, portanto, deve ser ajustado de acordo com o tamanho da rede a ser monitorada. O mais importante é ajustar as configurações de *backend*. Em seguida, adiciona-se a linha zabbix_server_enable = "YES" a /etc/rc.conf, que é o arquivo de configuração responsável por definir quais serviços devem ser inicializados junto com sistema operacional:

```
echo "zabbix_server_enable=\"YES\"" >> /etc/rc.conf
/usr/local/etc/rc.d/zabbix_server start
```

Configurando o agente do Zabbix: Primeiro é feita a instalação do Zabbix-Agent da porta do componente necessário para o correto funcionamento do agente no sistema que é o *pkgconf* (que é um programa que ajuda a configurar os sinalizadores do compilador e do *linker* para estruturas de desenvolvimento). Logo após, habilita-se o agente a ser iniciado junto com o sistema operacional, através do “rc.conf” e inicia-se o agente nos serviços individuais do sistema através do “rc.d”.

```
cd /usr/ports/net-mgmt/zabbix-agent
make install clean
echo "zabbix_agentd_enable=\"YES\"" >> /etc/rc.conf
/usr/local/etc/rc.d/zabbix_agentd start
```

E por último, é finalizada a configuração de *frontend*, que se inicia com a instalação das portas dos componentes dependentes para o correto funcionamento do *frontend*. Componentes esses que são: php, bcmath, ctype, sockets, mysqli entre outros.

```
cd /usr/ports/net-mgmt/zabbix-frontend
make install clean
```

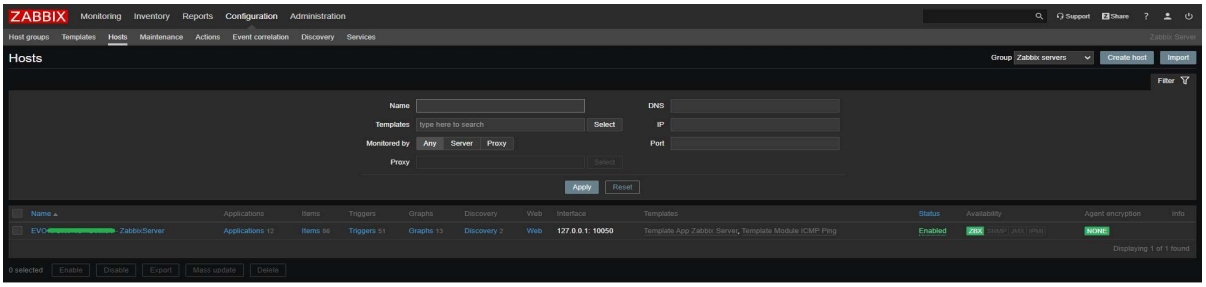
Logo após, já é possível acessar as configurações do Zabbix pelo navegador, através do endereço https://localhost/zabbix (ver Figura 15).

Figura 15 - Tela inicial do Zabbix Server

Fonte: (Autoria Própria)

Feitas estas configurações de instalação do Zabbix-Server, Zabbix-Agent e Zabbix-Frontend, necessárias para a correta operação da aplicação e os ajustes na *interface web* para se iniciar os monitoramentos, o primeiro dispositivo a ser monitorado foi inserido automaticamente pela instalação do Zabbix: o próprio Zabbix Server, com uma *template* também inserida por padrão automaticamente, conforme ilustrado na Figura 16.

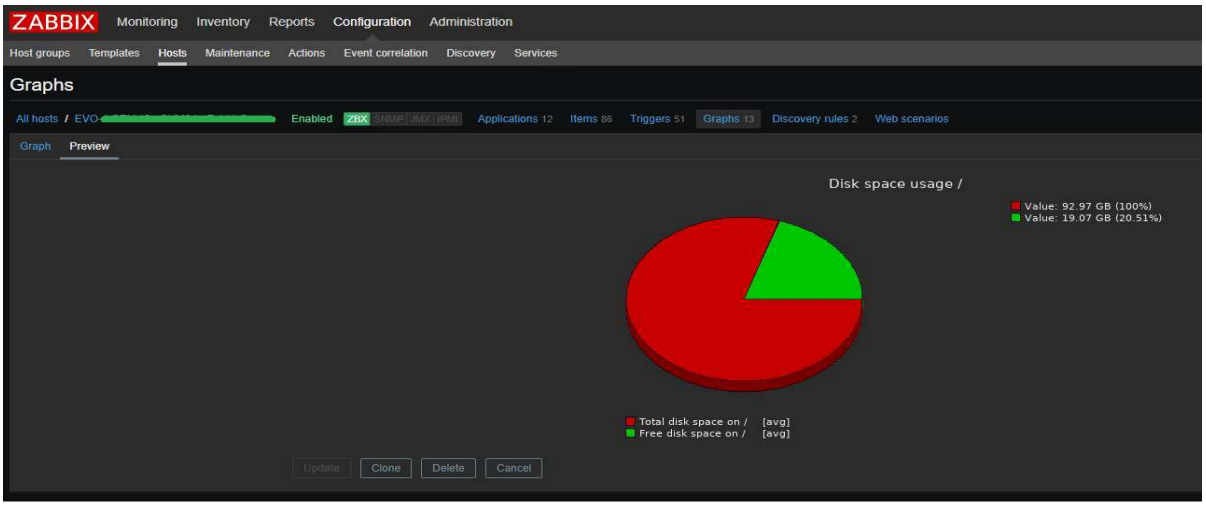
Figura 16 - Primeiro host a ser monitorado criado: o Zabbix Server



Fonte: (Autoria Própria)

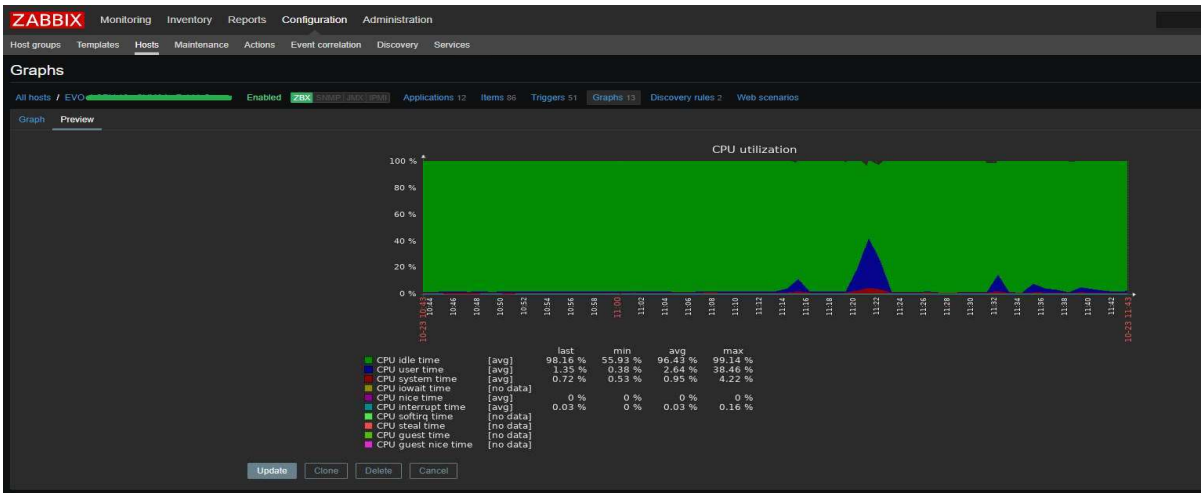
Dos itens monitorados presentes nas *templates*, destacam-se dois: o uso de disco, representado na Figura 17, e o uso de processador, mostrado na Figura 18.

Figura 17 - Uso de disco do Zabbix Server



Fonte: (Autoria Própria)

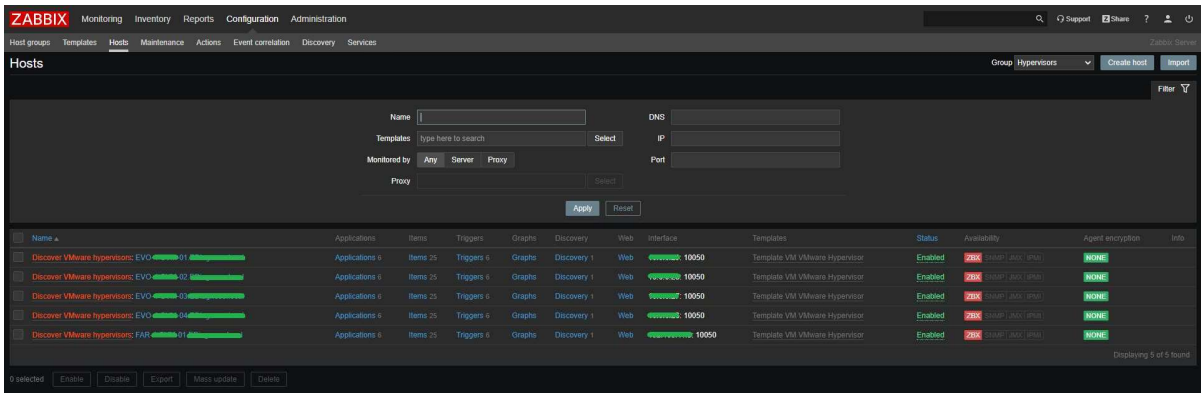
Figura 18 - Uso de processador do Zabbix Server



Fonte: (Autoria Própria)

Graças a VPN interligando as filiais à matriz, é possível monitorar todos os servidores da empresa. Desta forma, foram adicionados os servidores de virtualização (ver Figura 19). Quatro deles (localizados na matriz) estão em pleno funcionamento, o quinto, destinado a uma das filiais, está configurado com duas instâncias virtuais: uma para ser o controlador de domínio, e outra para o armazenamento de imagens, faltando apenas a migração dos dados dos antigos servidores físicos para esses servidores virtuais, para então, entrarem em produção. Por motivos de confidencialidade, foram suprimidos parte dos nomes dos hosts e seus endereços IP, visto que a empresa adota uma padronização de nomes baseada em *Netbios* para as máquinas, de maneira a identificá-las em quaisquer formas de registro.

Figura 19 - Servidores de virtualização equipados com o *software* VMWare



Fonte: (Autoria Própria)

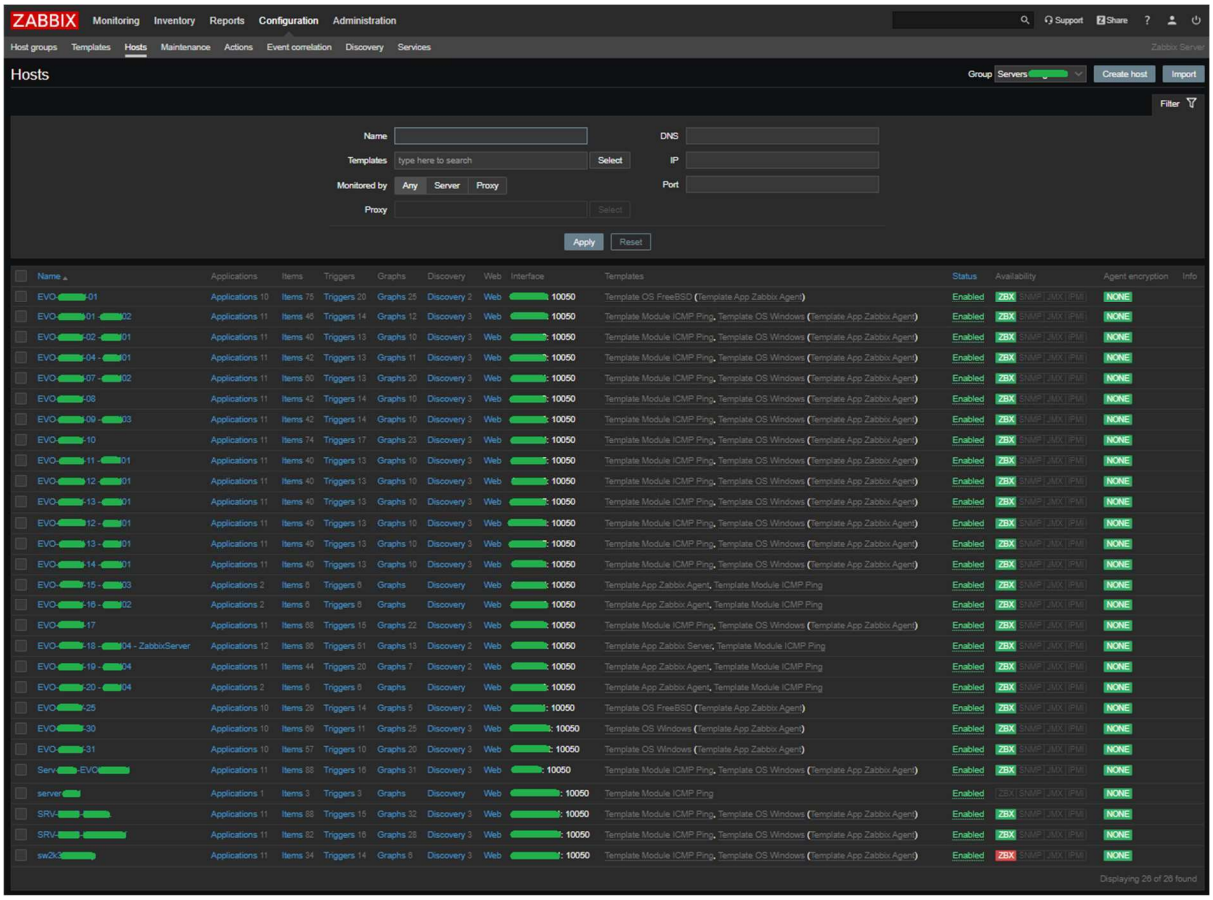
Aqui, além do uso de processador (item da aplicação CPU), destaca-se o uso de memória (item da aplicação *Memory*), conforme está na figura 20.

Figura 20 - Uso de memória de um dos servidores de virtualização

Fonte: (Autoria Própria)

Então, foi adicionada a maioria dos servidores que estão em produção atualmente: *firewall*, servidores *ERP*, servidores de imagem, servidor de backup etc. (ver Figura 21). Estão entre os servidores monitorados, tanto os virtuais quanto os servidores físicos.

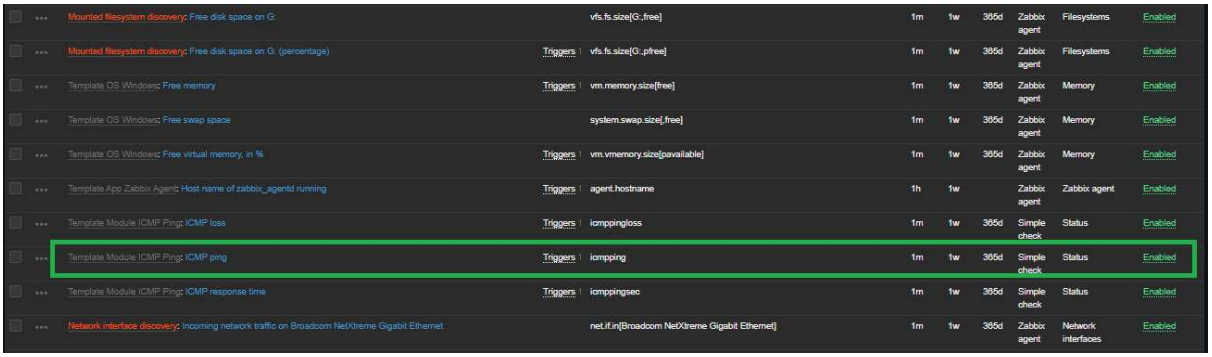
Figura 21 - Servidores monitorados



Fonte: (Autoria Própria)

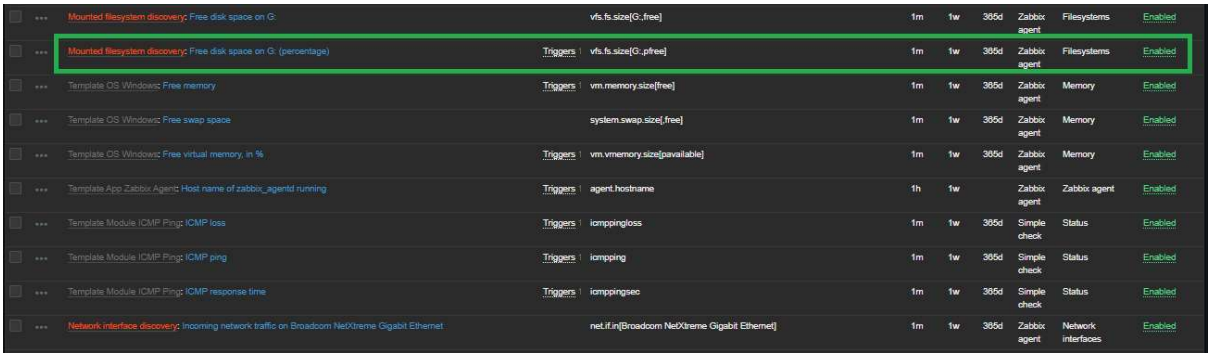
Dos servidores de imagem, é monitorado com maior cuidado a disponibilidade (item da aplicação *Status*), o espaço livre em disco (item da aplicação *Filesystems*) e o uso do processador (item da aplicação *CPU*), conforme consta nas Figuras 22, 23 e 24, respectivamente.

Figura 22 - Item disponibilidade do servidor de imagens



Fonte: (Autoria Própria)

Figura 23 - Item espaço livre em disco do servidor de imagem



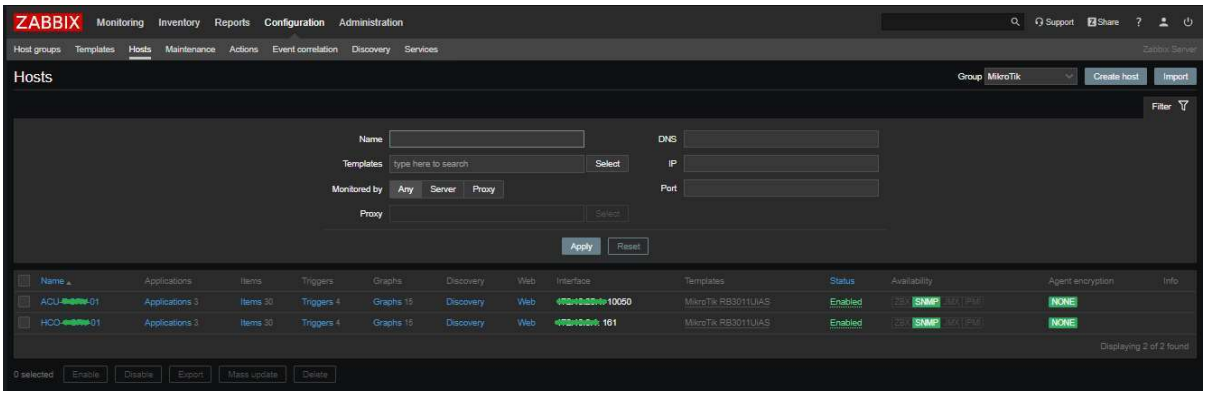
Fonte: (Autoria Própria)

Figura 24 - Item uso de processador do servidor de imagem

Fonte: (Autoria Própria)

Foram acrescentadas também no Zabbix, para monitoramento, dois roteadores, localizadas em duas das filiais (ver Figura 25). A Figura 26 ilustra o monitoramento de suas *interfaces* de comunicação, medindo o tráfego de entrada e saída de dados.

Figura 25 - Roteadores sendo monitorados



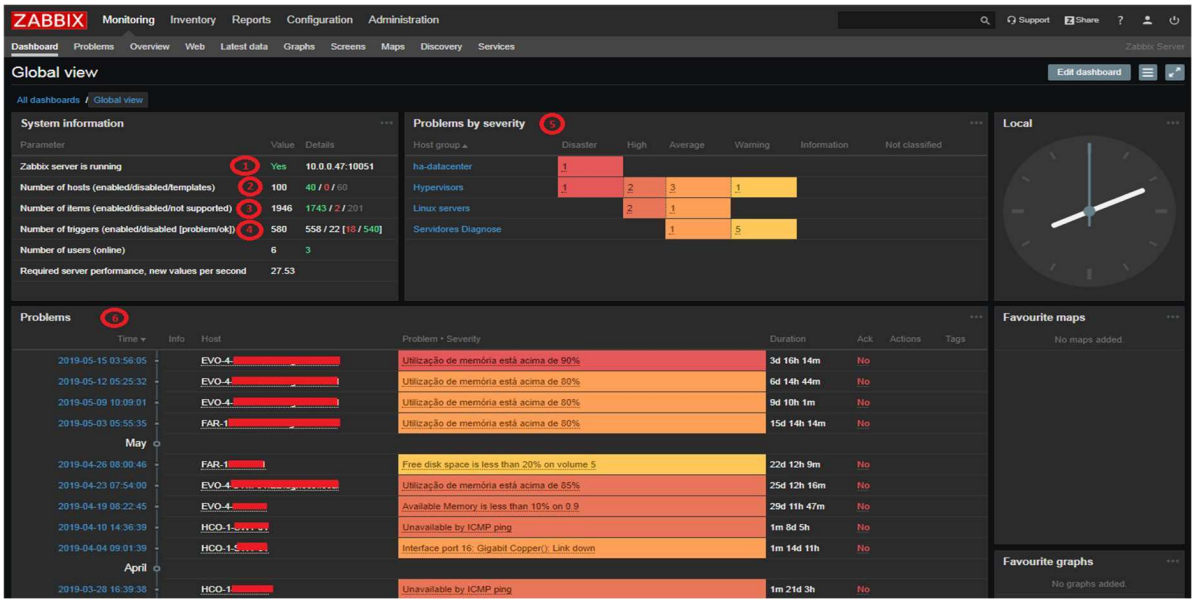
Fonte: (Autoria Própria)

Figura 26 - Interfaces de comunicação de um roteador

Fonte: (Autoria Própria)

Na Figura 27 é mostrada a tela inicial do Zabbix, com um resumo do ambiente de monitoramento englobando os equipamentos da matriz e das filiais, onde observa-se se o serviço do Zabbix está rodando efetivamente (1), o número de *hosts* monitorados (2), a quantidade de itens utilizados (3), a quantidade de *triggers* (4), a quantidade de problemas ativos separados por grupo de servidores (5) e o detalhamento desses problemas classificados por data e hora (6).

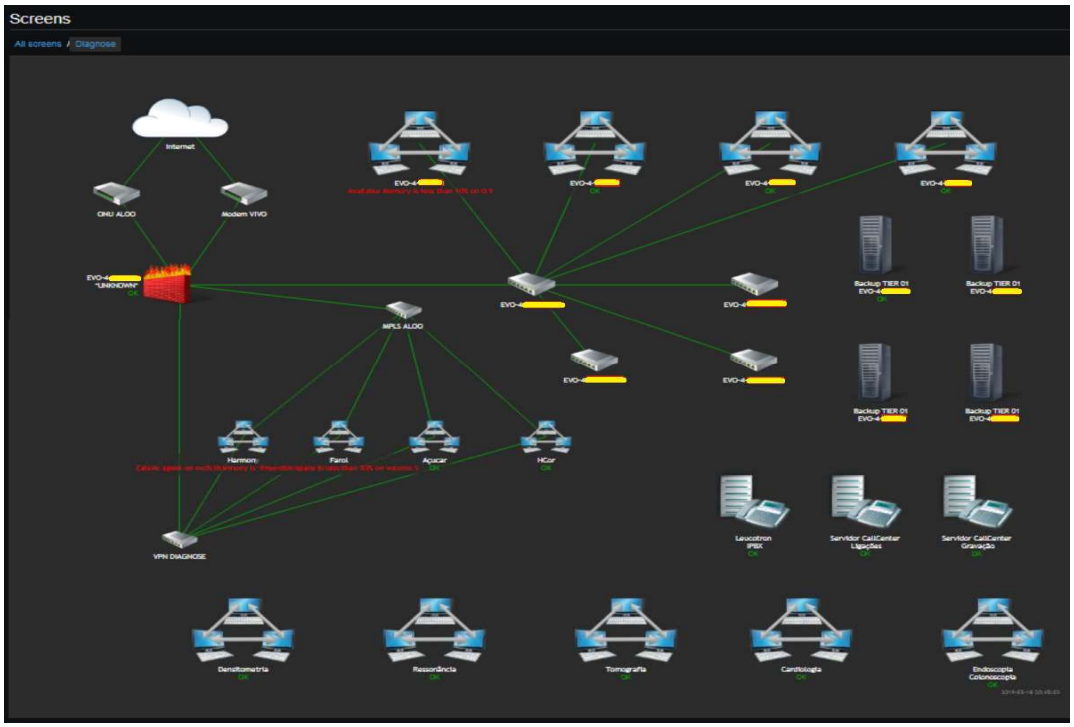
Figura 27 - Tela inicial do monitoramento com um breve resumo



Fonte: (Autoria Própria)

Em seguida, temos uma configuração feita com a opção Telas do Zabbix, onde se mostra um resumo dos *status* com o auxílio de ícones de rede (ver Figura 28). Nela, se observa o status dos servidores da matriz e das filiais, com a mensagem em vermelho indicando problemas.

Figura 28 - Status da rede apresentado de forma gráfica através da opção Telas do Zabbix



Fonte: (Autoria Própria)

Como visto, apesar do grande poder, quantidade e variedade de métricas do Zabbix, seus gráficos e telas são pouco atraentes aos olhos. Principalmente de pessoas estranhas ao setor de informática, como é o caso da alta gerência, que prefere algo mais simples e direto. É aí que entra a justificativa para se integrar o Grafana ao Zabbix. Na Figura 29 é ilustrado um painel visual com as principais métricas dos servidores mais importantes hoje para o negócio da empresa. Nele, além dos itens citados nos parágrafos anteriores, como disponibilidade, espaço livre em disco, uso de processador, uso de memória, foi acrescentado em forma de gráfico, o item leitura e escrita no disco dos servidores de imagem.

Figura 29 - Painel Visual Grafana e principais métricas de alguns servidores físicos e virtuais

Fonte: (Autoria Própria)

Utiliza-se dos gráficos e relatórios mais elegantes do Grafana para se montar e apresentar relatórios com um poder maior de convencimento para novos investimentos na área de informática da empresa, sempre buscando a segurança das informações sensíveis aos negócios.

Nas seções seguintes, serão detalhados alguns problemas comuns na empresa analisada neste trabalho, bem como apresentadas as soluções disponibilizadas pela adoção de um gerenciamento integrado, junto aos seus componentes da infraestrutura de Tecnologia da Informação.

6.3 Problema 1: Disponibilidade e Espaço em Disco dos Servidores de Imagem

A empresa conta, em sua matriz e em duas filiais, com servidores físicos dedicados ao armazenamento de imagens dos exames realizados, como por exemplo, de ressonância magnética, ultrassom e raios-X. Visto que as máquinas que realizam estes exames contam com poder de armazenamento limitado, um local de armazenamento como esse é essencial para a prestação do serviço aos clientes.

6.3.1 Situação antes da implantação

Não era raro ocorrer travamentos, lentidão ou desligamentos desses servidores. Travamentos do serviço eram também causados pelo esgotamento de espaço em disco. Apesar de certa frequência, a equipe de informática levava um certo tempo para, primeiramente, perceber que o problema estava ocorrendo. Podendo ser sentido apenas com um ou dois dias de atraso, a depender do caso, e depois, para identificar o real problema, pois, como as reclamações eram pontuais, se iniciava a investigação pelas estações de trabalho. Como o espaço de armazenamento dos servidores tem capacidade limitada, contando com no máximo 3 TB, é preciso manter o controle sobre o espaço disponível em cada servidor.

Em algumas situações, havia relatos de que o equipamento de exame não estaria conseguindo enviar as imagens para o servidor. Após a equipe de suporte investigar primeiramente o equipamento, se identificava que o real problema era que o espaço no servidor já não era suficiente. Isso ocasionava o acúmulo de imagens na estação de trabalho, acarretando lentidão na manipulação dos exames.

6.3.2 Situação depois da implantação

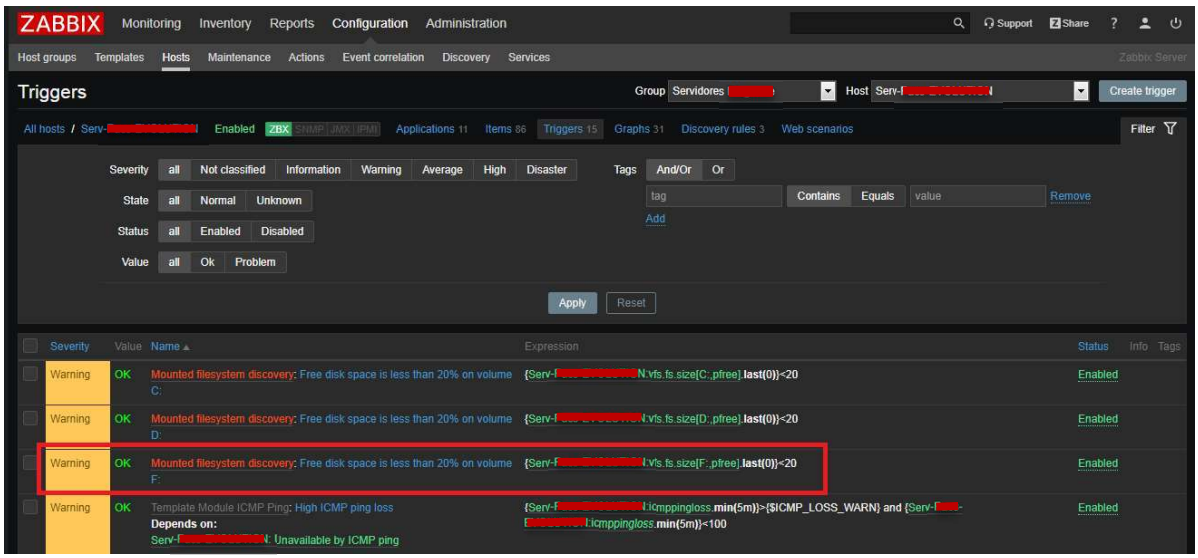
Para resolução deste problema, foi implementado o monitoramento do espaço em disco desses servidores, diminuindo assim, o tempo de reação e resolução de problemas futuros.

Para coletar as informações de todos os servidores foi instalado o Zabbix Agent em cada servidor, uma vez que é recomendado tê-lo instalado onde for possível, pois a quantidade de informações que podem ser coletadas e tabuladas para o Zabbix Server é muito grande.

O agente foi instalado seguindo o padrão, com as configurações mínimas para a correta troca de informações entre ele e o gerente. Desse modo, o agente envia por padrão, os dados solicitados pelo Zabbix Server a cada 60 segundos, uma vez que neste momento, para a empresa, não é necessário parâmetros mais elaborados.

Quando ocorrem situações limites, em relação às métricas de espaço de disco, disponibilidade, utilização de processador, acesso ao disco e memória disponível, são enviadas *triggers* para o Zabbix Server. Em especial ao armazenamento em disco, a mensagem de *trigger* é enviada no momento em que o espaço livre do disco atinge menos de 20%, com o grau de severidade definido em Atenção, conforme ilustrado na Figura 30.

Figura 30 - Trigger que dispara alerta para o Zabbix



Fonte: (Autoria Própria)

Estas configurações relacionadas às mensagens de *trigger*, hoje permitem que as equipes de informática se antecipem aos questionamentos de colaboradores da empresa. Uma vez que, o tempo definido para que o Zabbix dispare alertas sobre problemas graves (desastre) é de 2 minutos, e para serviços com uma tolerância maior de resolução é de 5 minutos.

Monitorando a disponibilidade, é possível identificar com maior facilidade possíveis travamentos do *hardware* ou do sistema operacional do servidor. E com o monitoramento do espaço em disco, é possível se antecipar à falta dele, e promover o remanejamento das imagens para um disco auxiliar de backup. Com isso, o que antes

se levava até dois dias para identificar a falha e se iniciar uma tratativa para solucionar o problema, hoje é resolvido de forma transparente para o colaborador. Ou seja, esse problema não é sentido, pois a falha não chega a ocorrer de fato.

6.4 Problema 2: Identificação de Melhorias Necessárias

O parque tecnológico de uma empresa deve estar em constante evolução, aprimorando seus serviços para proporcionar suporte ao negócio que move a empresa. Isso inclui a busca por melhores equipamentos e *softwares*, tanto para melhor proteção dos dados, quanto para a busca de um melhor desempenho da estrutura da rede.

6.4.1 Situação antes da implantação

Havia pouca ou nenhuma documentação sobre os equipamentos que compunham a rede, com equipamentos e *softwares* obsoletos. Não havia qualquer tipo de monitoramento, apenas uma incipiente implantação de um *firewall (PFSense)* e de um antivírus corporativo *(BitDefender)*.

Providências para melhoria só eram tomadas quando um equipamento em produção entrava em situação de parada definitiva. Fato que ocorreu por duas vezes em 2017, sendo um servidor de imagem e um *switch*, e outra vez em 2018 com outro servidor de imagem.

6.4.2 Situação depois da implantação

Com relatórios enriquecidos pelos gráficos do Grafana, a gerência de informática foi capaz de convencer a alta direção a adquirir equipamentos fundamentais. Como um servidor próprio para rodar o *firewall (ServerU),* em substituição a um PC comum que era encarregado de tal tarefa. Foi possível também conseguir a compra de um servidor de rack (1U) e dois novos *switches*, estes gerenciáveis, ao contrário dos antigos.

No fragmento de gráfico extraído do painel visual do Grafana, é possível ver que é iminente a necessidade de se investir em aquisição de mais memória para os servidores de virtualização, como mostra a Figura 31.

Figura 31 - Memória RAM dos servidores de virtualização próxima do colapso

Fonte: (Autoria Própria)

CAPÍTULO 7 - CONSIDERAÇÕES FINAIS

Atualmente, a premissa dominante em relação à informação é de que ela é fundamental, a matéria-prima das empresas, e que se deve tratá-la da forma correta para apoiar decisões acertadas e em tempo hábil. Essa responsabilidade recai sobre os ombros do setor de informática, já que cabe a este tomar decisões coerentes para minimizar desta forma, o *downtime* de ativos de rede e o tempo de ociosidade do colaborador que dependa de um sistema ou serviço específico.

Depois da implantação do ambiente de monitoramento Zabbix em conjunto com o Grafana, é possível citar algumas das importantes melhorias e benefícios percebidos após esse processo. Por exemplo, a agilidade em identificar problemas de disponibilidade em servidores, apontando um diagnóstico preciso de travamento, erro de disco ou super aquecimento. Facilidade em identificar e providenciar a liberação de espaço nos discos dos servidores, visto que eles ainda hoje possuem uma severa limitação de espaço. Com isso, foi possível a gerência do setor de informática elaborar um relatório apontando a necessidade de se adotar, em um futuro breve, uma Storage de discos para armazenamento das informações.

Então, pode-se afirmar que a solução conjunta atendeu às expectativas dos autores, solucionando os dois problemas propostos neste trabalho. Uma vez que, além da proatividade no quesito espaço em disco, evitando a parada na realização dos exames tão comum no passado, atualmente, com a ajuda dos relatórios elaborados pela solução por parte da gestão de TI, a diretoria entende, aceita e já planeja liberar recursos para a aquisição de uma *Storage* robusta, para o armazenamento de todas as imagens, de todos os exames realizados em todas as unidades da empresa. Isso por um prazo mínimo de 5 anos, e em alguns casos, até por 10 anos. Além de já ter investido em outras melhorias que foram mostradas também urgentes, como aquisição de novos *switches* gerenciáveis, novos servidores e melhoria de alguns mais antigos, mas que ainda possuem vida útil.

É possível afirmar também que a solução de monitoramento de rede Zabbix em conjunto com os gráficos do Grafana, tem potencial para possibilitar a qualquer equipe gestora de informática, quer seja de uma pequena, média ou grande empresa, uma maior facilidade no gerenciamento dos equipamentos, serviços e sistema. Isso, devido ao fato de que a configuração das mensagens de alertas para incidentes

proporciona segurança, celeridade e o mais importante, a manutenção preventiva por parte da equipe responsável.

Como trabalhos futuros, sugerimos alguns que se mostraram interessantes durante a elaboração deste trabalho. Como por exemplo, a integração do Zabbix com o GLPI (abertura de chamados) ou outro compatível, onde é possível fazer com que o Zabbix abra um chamado automaticamente ao identificar algum problema em um dispositivo de rede. Também, a possibilidade de integração do Zabbix com o OCS Inventory[6], para um melhor controle do inventário de máquinas. Além da implementação de envio de alertas por e-mail, SMS, ligações e pelo mensageiro Telegram. Sobre este último não houve tempo hábil para implantação e inclusão neste trabalho.

[6] *Software* livre que permite aos usuários inventariar ativos de TI. Site oficial: https://ocsinventory-ng.org

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, F. R.; PIRES H. D. **Gerência de redes**. Trabalho de Conclusão de Curso (Graduação em Engenharia de Telecomunicações) – Departamento de Engenharia de Telecomunicações, Universidade Federal Fluminense, Niterói, Rio de Janeiro, p. 25. 2014. Disponível em: <https://fdocumentos.tips/document/gerencia-de-redes-de-boraredes1pdftrab042snmppdf-departamento-de-engenharia.html>. Acesso em: 10 jul. 2020.

ALVES, Kedson. Gestão de Indicadores/Métricas com Grafana. **Profissionais TI**, 2018. Disponível em <https://www.profissionaisti.com.br/2018/10/gestao-de-indicadoresmetricas-com-grafana>. Acesso em: 11 de maio 2019.

AMARAL, M. C. do. **REASON - Avaliação de confiabilidade e disponibilidade em redes de computadores sustentáveis**. Dissertação (Mestrado em Engenharia Elétrica), Escola Politécnica da Universidade de São Paulo, São Paulo, p. 134. 2014. Disponível em <http://www.lassu.usp.br/lassu/wp-content/uploads/2016/08/marcelo_diss.pdf>. Acesso em: 20 de jan. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 5462: Confiabilidade e mantenabilidade**. Rio de Janeiro. 1994.

BAHALS, A. **Monitoramento Proativo do Ambiente de Rede Utilizando o Software Zabbix**. Trabalho de Conclusão de Curso (Tecnológico em Análise e Desenvolvimento de Sistemas) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Ponta Grossa, p. 64. 2016. Disponível em <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/7417/1/PG_COADS_2016_1_01.pdf>. Acesso em: 28 de mar. 2020.

BENÍCIO, W. E. P. **Monitoramento e Gerenciamento de Redes Utilizando Zabbix**. Trabalho de Conclusão de Curso (Tecnológico em Análise e Desenvolvimento de

Sistemas) - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Capivari, p. 72. 2015. Disponível em <http://zabbixbrasil.org/files/Monitoramento_e_Gerenciamento_de_Redes_Utilizando_Zabbix.pdf>. Acesso em: 11 de maio 2019.

BONOMO, E. **Gerenciamento e Monitoração de Redes de Computadores Utilizando-se Zabbix**. Monografia (Pós-Graduação Lato Sensu em Administração de Redes Linux) - Departamento de Pós-Graduação, Universidade Federal de Lavras, Minas Gerais, p. 67. 2006. Disponível em: <http://repositorio.ufla.br/jspui/bitstream/1/9373/1/MONOGRAFIA_Gerenciamento%20e%20monitora%C3%A7%C3%A3o%20de%20redes%20de%20computadores%20utilizando-se%20Zabbix.pdf>. Acesso em: 6 de maio 2020.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Institui Lei a Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, n. 157, p. 59, 15 ago. 2018.

BUENO, E. M. **Monitoramento de redes de computadores com uso de ferramentas de software livre**. Monografia (Curso de especialização software livre aplicado à telemática) - Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, p. 73. 2012. Disponível em <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1842/1/CT_CESOL_I_2012_05.pdf>. Acesso em: 07 de maio 2020.

CASE, J.; FEDOR, M.; SCHOFFSTALL, M.; DAVIN, J. **A Simple Network Management Protocol (SNMP)**. IETF - RFC 1157, May 1990.

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

COMER, Douglas E. **Interligação de redes com TCP/IP: Princípios, protocolos e arquitetura**. 6ª edição. Rio de Janeiro: Campus, 2015.

CONTESSA, D. F.; POLINA, E. R. Gerenciamento de Equipamentos Usando o Protocolo SNMP. **CP Eletrônica S.A.**, [s.d.]. Disponível em <http://paginas.unisul.br/carlos.luz/admredes/unidade1/ArtigoSNMP.pdf>. Acesso em: 4 de maio 2019.

DIAS, Beethovem Zanella; ALVES Jr., Nilton. **Protocolo de Gerenciamento SNMP**, CBPF - NT-006/01, Rio de Janeiro, 2002.

ELER, Esdras de Oliveira. Modelo TMN: Aplicação ao Gerenciamento de Redes de Telecomunicações. **Teleco**, 2015. Disponível em <https://www.teleco.com.br/tutoriais/tutorialmodelotmn/default.asp>. Acesso em: 13 de fev. 2020.

FERNANDES, Í. F. **Proposta de utilização da ferramenta Zabbix no gerenciamento de redes: Um Estudo de Caso no Ambiente da FAB Segundo Boas Práticas de Governança de TI**. Monografia (Pós-Graduação em Gerência de Redes de Computadores e Tecnologia Internet) – Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro, Rio de Janeiro, p. 58. 2013. Disponível em: <https://pantheon.ufrj.br/bitstream/11422/3300/4/IAguiar.pdf>. Acesso em: 30 de mar. 2020.

FILHO. A. G.; GEREMIAS, J. **Avaliação da Ferramenta Zabbix**. Trabalho de Conclusão de Curso (Especialização em Redes e Segurança de Sistemas) – Pontifícia Universidade Católica do Paraná, Curitiba, p. 34. 2010. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Adilson%20Galiano%20-%20Artigo.pdf>. Acesso em: 30 de mar. 2020.

GONÇALVES, Marcus. **Firewalls Guia Completo**. Rio de Janeiro: Ciência Moderna, 2000.

GUILLERMO, O. E. P. **Uso de Agentes SNMP para monitoramento de Servidores e equipamentos de rede com mobilidade**. Trabalho de Conclusão de Curso (Especialista em Tecnologias, Gerência e Segurança de Redes de Computadores) – Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, p. 71.

2008. Disponível em <https://www.lume.ufrgs.br/bitstream/handle/10183/15981/000695294.pdf?sequence=1>. Acesso em: 13 de fev. 2020.

HENRIQUE, Marcos. **Nagios - Monitorando Redes Corporativas**. 1ª Edição. Rio de Janeiro: Ciência Moderna, 2014.

HORST, Adail Spínola; PIRES, Aécio dos Santos; DEÓ, André L. Boni. **De A a Zabbix**. São Paulo: Novatec, 2015.

JEE, Charlotte; MACAULAY, Thomas. 10 grandes falhas da tecnologia nos últimos anos. **Computerworld**, São Paulo, 2018. Disponível em: <https://computerworld.com.br/2018/07/12/10-grandes-falhas-da-tecnologia-nos-ultimos-anos/>. Acesso em: 12 de set. 2020.

KUROSE, Ross. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 5ª Edição. São Paulo: Pearson, 2010.

LASKOSKI, Jackson. Monitorando Redes com o The Dude. **Linha de Código**, [20-]. Disponível em <http://www.linhadecodigo.com.br/artigo/3287/monitorando-redes-com-o-the-dude.aspx>. Acesso em: 08 de dez. 2019.

LIMA, Janssen dos Reis. **Monitoramento de Redes com Zabbix: Monitore a saúde dos servidores e equipamentos de redes**. Rio de Janeiro: Brasport, 2014.

MACÊDO, Diego. Enumeração com SNMP. **Diego Macêdo: Um pouco de tudo sobre TI**, 2017. Disponível em <https://www.diegomacedo.com.br/enumeracao-com-snmp/>. Acesso em: 19 de maio 2019.

MAURO, Douglas R.; SCHMIDT, Kevin J. **SNMP Essencial: Ajuda para os Administradores de Sistemas e de Redes**. Rio de Janeiro: Campus, 2001.

MCCLOGHRIE K.; ROSE M. **Management Information Base for Network Management of TCP/IP-based internets**. IETF - RFC 1066, August 1988.

MCCLOGHRIE K.; ROSE M. **Management Information Base for Network Management of TCP/IP-based internets: MIB-II**. IETF - RFC 1213, March 1991.

MONITORAMENTO de rede: entenda por que ele é fundamental para sua empresa. **Tecnojump**, Florianópolis, 2017. Disponível em <https://blog.tecjump.com.br/monitoramento-de-rede-entenda-por-que-ele-e-fundamental-para-sua-empresa/>. Acesso em: 12 de set. 2020.

OLIVEIRA, A. S.; LIMA, P. A. **Integração do Framework de Monitoramento Zabbix com uma Nuvem Privada**. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdade de Computação, Universidade Federal do Pará, Marabá, p. 82. 2013. Disponível em: <https://faceel.unifesspa.edu.br/images/works/TCC/2013/INTEGRACAO-DO-FRAMEWORK-DE-MONITORAMENTO-ZABBIX-COM-UMA-NUVEM-PRIVADA.pdf>. Acesso em: 30 de mar. 2020.

OLIVEIRA, José Mário; LINS, Rafael Dueire; MENDONÇA, Roberto. **REDES MPLS: Fundamentos e Aplicações**. 1ª edição. São Paulo. Brasport, 2012.

PINHEIRO, José Maurício Santos. O MPLS em Redes de Computadores. **Projeto de Redes**, 2006. Disponível em <https://www.projetoderedes.com.br/artigos/artigo_mpls_em_redes.php>. Acesso em: 19 de maio 2019.

PINHEIRO, Ricardo. O protocolo SNMP. **CooperaTI**, 2011. Disponível em <https://cooperati.com.br/2011/09/o-protocolo-snmp/>. Acesso em: 12 de set. 2020.

PIRES, Aécio. Integração do Zabbix com Grafana. **Zabbixbrasil.org**, 2019. Disponível em <http://zabbixbrasil.org/?p=1674>. Acesso em: 12 de set. 2020.

SALITURO, Eric. **Learn Grafana 7.0: A beginner's guide to getting well versed in analytics, interactive dashboards, and monitoring**. 1ª Edição. Birmingham: Packt Publishing, 2020.

SETE falhas tecnológicas que causaram prejuízos para empresas e usuários. **33Giga**, 2019. Disponível em <https://33giga.com.br/7-falhas-tecnologicas-que-causaram-prejuizos-para-empresas-e-usuarios/>. Acesso em: 12 de set. 2020.

SILVA, J. M. A. da. **Construção de Agentes SNMP**. Monografia (Pós-Graduação em Administração em Redes Linux) – Departamento de Ciência da Computação, Universidade Federal de Lavras, Minas Gerais, p. 114. 2005. Disponível em <https://issuu.com/arlufla/docs/mono-josesilva>. Acesso em: 04 de maio 2019.

SISU 2019 recebe 10 vezes mais acessos do que o esperado e site fica instável. **G1**, 2019. Disponível em: <https://g1.globo.com/educacao/guia-de-carreiras/noticia/2019/01/23/sisu-2019-recebe-10-vezes-mais-acessos-do-que-o-esperado-e-site-fica-instavel.ghtml>. Acesso em: 20 de jun. de 2020.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2**. Third Edition. Massachusetts: Addison-Wesley, 1999.

TANENBAUM, Andrew S. **Redes de Computadores**. 4ª Edição. Rio de Janeiro: Campus, 2003.

TERPLAN, Kornel. **Web-based Systems and Network Management**. 1ª Edição. Florida: CRC Press, 1999.

ZABBIX SIA (Japão) (org.). **Zabbix Documentation 4.0**. 2018. Disponível em <https://www.zabbix.com/documentation/4.0/pt/manual>. Acesso em: 15 de dez. 2019.

ZARPELÃO, Bruno Bogaz. SNMP: Simple Network Management Protocol - Revista Infra Magazine 7. **DEVMEDIA**, 2012. Disponível em < https://www.devmedia.com.br/snmp-simple-network-management-protocol-revista-infra-magazine-7/25683>. Acesso em: 25 de nov. 2020.

ZOBNIN, Alexander. **About Grafana-Zabbix plugin**, 2015. Disponível em: <https://alexanderzobnin.github.io/grafana-zabbix/>. Acesso em: 20 de maio 2020.