UNIVERSIDADE DO ESTADO DO RIO GRANDE NO NORTE – UERN
FACULDADE DE CIÊNCIAS EXATAS E NATURAIS – FANAT
DEPARTAMENTO DE INFORMÁTICA – DI

FRANCISCO MARCOS DA COSTA MONTEIRO

ESTUDO, ANÁLISE E IMPLEMENTAÇÃO DE UM NETWORK OPERATIONS CENTER NO LABORATÓRIO DE ENSINO E PESQUISA DE REDES DE COMPUTADORES.

MOSSORÓ - RN
2022

FRANCISCO MARCOS DA COSTA MONTEIRO

ESTUDO, ANÁLISE E IMPLEMENTAÇÃO DE UM NETWORK OPERATIONS CENTER NO LABORATÓRIO DE ENSINO E PESQUISA DE REDES DE COMPUTADORES.

Monografia apresentada à Universidade do Estado do Rio Grande do Norte como um dos pré-requisitos para obtenção do grau de bacharel em Ciência da Computação, sob orientação do Prof. Dr. Rommel Wladimir de Lima

Aprovada em: 27/04/2022

Banca Examinadora

Prof. Dr. Rommel Wladimir de Lima
Universidade do Estado do Rio Grande do Norte - UERN

Prof. Dr. Sebastião Emídio Alves Filho
Universidade do Estado do Rio Grande do Norte - UERN

Prof. Dr. Isaac de Lima Oliveira Filho
Universidade do Estado do Rio Grande do Norte - UERN

AGRADECIMENTOS

Primeiramente agradeço a Deus pela vida que me foi concedida, saúde e força de vontade, que não me permitiu desistir.

Agradeço imensamente aos meus pais, Maria da Saúde e Francisco Carlos, que me apoiaram durante toda a jornada, sem eles eu não teria conseguido.

Aos meus irmãos, Antonio Maxwell e Lara Fabia, que me deram forças e tanto me ajudaram durante esse tempo.

Sou muito grato ao meu orientador, Prof. Rommel Wladimir de Lima, que aceitou este desafio e por toda contribuição para o desenvolvimento deste projeto.

Aos meus amigos de faculdade, por contribuírem com minha formação e por todas as resenhas, risadas e bons momentos que ficaram gravados para sempre em meu coração.

Ao pessoal do ônibus, em especial a Márcio, por toda ajuda que me deu ao longo dos primeiros semestres.

A Mizael que é o técnico do laboratório, pela ajuda e suporte no desenvolvimento deste trabalho.

Ao pessoal da APDA em especial a Nêmora, Neneinha e Regina, que me ajudaram a conseguir o transporte adaptado.

“Enquanto minha mente tiver asas, quero voar.”

- Stephen King

RESUMO

A popularização da Internet e tecnologias de redes de computadores, estão tão integradas na sociedade que é praticamente impossível realizar algumas atividades cotidianas, sem fazer uso das mesmas. Nesse caso, o gerenciamento e o controle da rede são cruciais, para planejar, supervisionar e controlar as atividades da rede, buscando garantir a disponibilidade e qualidade dos serviços. O projeto visa desenvolver um *Network Operations Center* - NOC - para o Laboratório de Redes e Sistemas Distribuídos – LORDI, para monitoramento de alguns dos equipamentos do Departamento de Informática da Universidade do Estado do Rio Grande do Norte. Para isso foi realizado um estudo e análise de requisitos, das ferramentas que efetuam a coleta automatizada dos dados da rede. Todo o processo de instalação, configuração e testes foram realizados em um ambiente controlado, iniciando pelo monitoramento de máquinas virtuais. Em seguida se expandiu para o monitoramento de diversos *hosts* dos laboratórios.

Palavras-chave: NOC, monitoramento, gerenciamento, Zabbix.

ABSTRACT

The popularization of the Internet and computer network technologies are so integrated into society that it is practically impossible to carry out some daily activities without making use of them. In this case, network management and control are crucial to plan, supervise and control network activities, seeking to guarantee the availability and quality of services. The project aims to develop a Network Operations Center - NOC - for the Laboratory of Networks and Distributed Systems - LORDI, to monitor some of the equipment of the Department of Informatics of the University of the State of Rio Grande do Norte. For this, a study and analysis of requirements was carried out, of the tools that perform the automated collection of network data. The entire installation, configuration and testing process was carried out in a controlled environment, starting with the monitoring of virtual machines. It then expanded to monitoring multiple lab hosts.

Keywords: NOC, monitoramento, gerenciamento, Zabbix.

LISTA DE SIGLAS

CGI	-	*Common Gateway Interface*
CPU	-	Unidade de Central de Processamento
DI	-	Departamento de Informática
FAQ	-	*Frequently Asked Questions*
GES	-	Grupo de Engenharia de Software
GPL	-	*General Public License*
HTML	-	*HyperText Markup Language*
HTTP	-	*Hypertext Transfer Protocol*
IETF	-	*Internet Engineering Task Force*
IP	-	*Internet Protocol*
IPS	-	Sistema de Prevenção de Instrução
LEC	-	Laboratório de Ensino de Computação
LORDI	-	Laboratório de Redes e Sistemas Distribuídos
MRTG	-	*Multi Router Traffic Grapher*
NNTP	-	*Network News Transfer Protocol*
NOC	-	*Network Operations Center*
POP3	-	*Post Office Protocol*
RFC	-	*Request for Comments*
SMTP	-	*Simple Mail Transfer Protocol*
SNMP	-	*Simple Network Management Protocol*
TCP	-	*Transmission Control Protocol*

TI	-	Tecnologia da Informação
UERN	-	Universidade do Estado do Rio Grande do Norte
URL	-	*Uniform Resource Locator*
UDP	-	Protocolo de datagrama do usuário
IPS	-	*Intrusion Prevention System*

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

O advento das redes de computadores e a popularização da internet, promoveu mudanças comportamentais significativas em nossa sociedade. Uma das tecnologias que mais tem colaborado com isso é a Internet, que pode ser definida como um conjunto de protocolos que possibilita a interligação de diferentes tecnologias de Redes de Computadores. Nesse contexto, no cerne da Internet estão os conceitos de redes de computadores, um conjunto de protocolos que possibilita a troca de informação entre dispositivos computacionais (KUROSE, 2007).

As redes de computadores são fruto de pesquisas militares, desenvolvidas durante a guerra fria. Inicialmente essas redes tornaram possível a comunicação entre organizações governamentais e universidades. No entanto, a rápida evolução das tecnologias de rede, aliada à grande redução no custo dos recursos computacionais, motivou a proliferação das redes de computadores em todos os segmentos da sociedade. Atualmente, as redes fazem parte do cotidiano das pessoas como uma ferramenta que oferece recursos e serviços, permitindo uma maior interação entre os usuários e consequente aumento da produtividade.

Nas últimas décadas, ocorreram mudanças significativas nos serviços ofertados através da rede, além dos novos, tais como redes sociais, internet das coisas e aplicações multimídia como streaming de filmes, músicas e até mesmo jogos. Também existe a crescente quantidade de dispositivos conectados à rede, aumentando ainda mais a complexidade das mesmas, tudo isso pode gerar uma série de problemas, como, indisponibilidade de serviços, quedas de links, falhas e etc.

Com isso surge a necessidade de gerenciar essas redes, para garantir seu pleno funcionamento. A gestão está associada às atividades de controle e monitoramento da utilização dos recursos no ambiente de rede. Esse trabalho é muito exaustivo para ser feito de forma manual, por isso existem diversas ferramentas criadas com essa finalidade.

Assim, a gestão de redes é o meio pelo qual é utilizado um conjunto de ferramentas, normalmente composto por uma solução de hardware e software que permite uma gestão centralizada e mais eficaz. Ela pode gerar dados históricos e

estatísticos a partir de seu ambiente computacional, além de atuar de forma mais assertiva em um momento de falha ou indisponibilidade.

1.1. Objetivos

1.1.1. Geral

Esse projeto tem como objetivo principal, realizar um estudo e análise para implementação de um *Network Operations Center* - NOC, no Laboratório de Redes e Sistemas Distribuídos - LORDI, através da ferramenta de gerenciamento de redes, Zabbix. O NOC será responsável por monitorar os servidores, páginas *web* e alguns *hosts* dos laboratórios do Departamento de Informática - DI - da Universidade do Estado do Rio Grande do Norte - UERN.

1.1.2. Específicos

- Estudar as ferramentas de gerenciamento existentes;
- Identificar, dentro das soluções estudadas, a que melhor se adequa a realidade do LORDI e LEC;
- Monitorar os *sites* dos laboratórios;
- Monitoramento dos computadores do Laboratório de Ensino de Computação - LEC;
- Configurar a ferramenta para enviar as notificações via Telegram;
- Desenvolver material de treinamento e tutoriais.

1.2. Metodologia

Este trabalho teve como finalidade a realização de um estudo com o objetivo de compreender o funcionamento do gerenciamento de redes e do NOC. Onde foi descoberto que para iniciar, era necessário entender bem os ambientes que estava sendo iniciado o monitorados, neste caso o Laboratório de Redes e Sistemas Distribuídos – LORDI - e o Laboratório de Ensino de Computação - LEC - para em seguida escolher a ferramenta de gerenciamento.

Neste sentido, a metodologia envolve a realização de um estudo da infraestrutura de rede do LORDI e LEC, buscando identificar os componentes, recursos e serviços disponibilizados pela rede.

Também foi feita uma pesquisa bibliográfica e documental, com abordagem quantitativa e qualitativa, com o intuito de aprender um pouco mais sobre redes de computadores, como criar um *Network Operation Center - NOC* - e identificar as ferramentas de gerenciamento de redes mais populares do mercado.

Após o levantamento bibliográfico, foi pesquisado sobre as diferentes ferramentas de gerenciamento de redes, com o objetivo de identificar a mais adequada para os laboratórios.

Na pesquisa experimental, foi realizada uma análise de requisitos, com o objetivo de entender o funcionamento do sistema, para desenvolver os tutoriais de instalação do Zabbix Server e Zabbix Agent. Em seguida a ferramenta foi instalada, foram feitas as configurações iniciais, instalação de agentes nos *hosts* dos laboratórios e organização da estrutura física do NOC.

Por fim, todos os dados analisados foram transformados em tutoriais, para facilitar a compreensão das funcionalidades da ferramenta e ajudar nas atualizações futuras.

1.3. Estrutura do trabalho

O trabalho está organizado da seguinte forma:

No capítulo 2 é apresentada a definição e contextualização de gerenciamento de redes e NOC.

No capítulo 3 é apresentado sobre o protocolo de gerenciamento de redes, abordando sobre sua definição, arquitetura e principais operações.

No capítulo 4 são apresentadas algumas das principais ferramentas de gerenciamento de redes, destacando os pontos positivos e negativos de cada uma.

No capítulo 5 É apresentada a definição e características do Network Operations Center

No capítulo 6 detalha o desenvolvimento do projeto, iniciando pela escolha da ferramenta, até a instalação e configurações iniciais da ferramenta.

No capítulo 7 para finalizar, são apresentadas as considerações finais, com as principais dificuldades encontradas durante o desenvolvimento do projeto e algumas propostas para possíveis trabalhos futuros.

2. GERENCIAMENTO DE REDES DE COMPUTADORES

2.1. Contextualização

Atualmente incontáveis serviços são prestados através da internet, tornando-se fundamental garantir não somente uma boa conexão mas também a qualidade dos serviços. Por isso torna-se tão importante obter as informações dessas redes, para fazer seu gerenciamento.

É possível entender a importância do monitoramento, através uma analogia simples. Atualmente muita gente usa as *smartbands*, que são pulseiras que coletam informações do estado de saúde do indivíduo, e enviam para um dispositivo como *smartphone* ou tablet, permitindo que a pessoa monitore seu estado de saúde, bem como manter um histórico dos dados monitorados. No ambiente das redes, o monitoramento acontece de forma semelhante, para fazer o gerenciamento, são necessárias um conjunto eficiente de ferramentas automatizadas, sendo fundamental a utilização de técnicas padronizadas para a correta representação e o intercâmbio das informações obtidas.

Assim o corpo humano será semelhante a infraestrutura de TI (*hosts*), as funções do corpo são como os serviços ofertados pelas redes, o *smartband* vai funcionar como um *software* (agente) que é usado para coletar dados. O *smartphone* ou tablet é como um *software* gerente, que trata e apresenta as informações (gerente). A Figura 1 apresenta uma analogia entre esses elementos.

Figura 1 - Analogia ao monitoramento de redes

Fonte: Autoria Própria.

Nesse contexto, surge o conceito de gerenciamento de redes, para Matos (2009) o gerenciamento de redes surge com o objetivo de planejar o crescimento, efetuar o monitoramento e proporcionar uma alta disponibilidade dos recursos da rede.

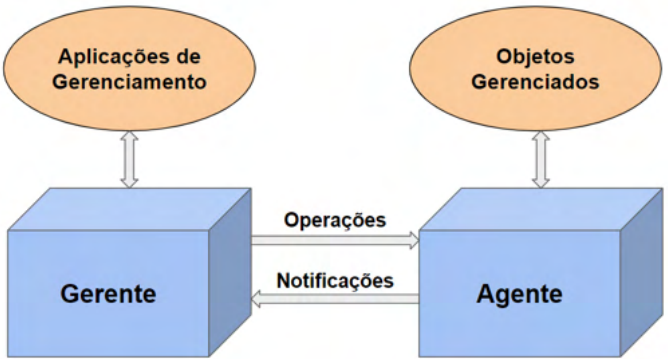
Obviamente, existe algum custo na gestão de redes, assim essa gestão é mais indicada para instituições públicas ou privadas que prestam serviços importantes, que precisam funcionar corretamente de forma constante.

2.2. Infraestrutura

O gerenciamento possui organizações, métodos, tecnologia e padrões próprios, segundo Benício (2015) “Monitorar uma rede é verificar a eficácia do funcionamento de cada serviço, equipamento e processos existentes em uma mesma infraestrutura”. Assim, analisar partes isoladas do sistema, pode não atender às necessidades de operação e manutenção dos mesmos.

É importante salientar que quando falamos em monitoramento de redes, não utilizamos os termos cliente e servidor, os termos amplamente difundidos são gerente e agente, conforme mostra a figura 2 que ilustra a estrutura básica do modelo de gerenciamento gerente/agente.

Figura 2 - Modelo de Gerenciamento: Gerente e Agente.



Fonte - PINHEIRO, 2006.

Os elementos envolvidos são:

- **Gerente:** O computador que possui o *software* de gerenciamento de rede;
- **Agente:** Faz a coleta e mantém a base com dados a serem consultados pelo gerente;

- **Objeto gerenciado**: São todos os objetos que podem ser monitorados, dentro de uma rede, possibilitando verificar certos parâmetros de funcionamento;
- **Aplicações de Gerenciamento:** Consiste em um conjunto de ferramentas, que fornecem um conjunto de dados coletados, além de emitirem alertas informando erros.

O gerenciamento de redes de computadores, trabalha tendo como base os três seguintes pilares:

- **Coleta de dados (*pooling*):** A coleta é realizada por componentes de *hardware* e *software*, que realiza uma bateria de coleta, no tempo determinado pelo administrador;
- **Análise:** Realiza a análise dos dados coletados e faz a inferência usando os parâmetros definidos pelo administrador da rede, assim será possível determinar, se os dados estão dentro ou fora da faixa normal esperada pelo administrador;
- **Ação:** Após a análise, algumas ações podem ser executadas nesta etapa. Por exemplo, uma ação pode ser um alerta visual em uma interface de navegador da *Web*, o envio de um e-mail ou qualquer ação suportada por uma plataforma conveniente e gerenciada.

2.3. Áreas

A *International Organization for Standardization* - ISO[1] - criou um modelo de gerenciamento de rede que apresenta de forma estruturada os cenários de gerenciamento, sendo dividido em cinco áreas.

Gerenciamento de desempenho: Sua meta é quantificar, notificar, analisar e controlar o desempenho dos ativos de TI que compõem a rede.
Gerenciamento de falhas: Tem como objetivo detectar, registrar e reagir em caso de falhas na rede, se difere do gerenciamento de desempenho, por adotar uma

[1] Também conhecida como Organização Internacional de Normalização – ISO – Seu objetivo é promover o desenvolvimento de normas, testes e certificações na área de Tecnologia da Informação.

estratégia de gerenciamento de longo prazo, em face de demandas variáveis de tráfego e falhas ocasionais na rede.

Gerenciamento de configuração: Permite saber a quantidade de dispositivos conectados à rede, bem como suas configurações de *hardware* e *software.*

Gerenciamento de contabilização: Permite aos administradores de rede especificar, registrar e controlar o acesso de usuários e dispositivos aos recursos da rede.

Gerenciamento de segurança: Seu objetivo é controlar o acesso aos recursos da rede de acordo com algumas políticas bem definidas. Esse tipo de gerenciamento busca garantir alta visibilidade do comportamento da rede, automatizar a configuração do dispositivo, aplicar políticas globais, visualizar o tráfego entre *firewalls*, gerar relatórios e fornecer uma interface de gerenciamento única para sistemas físicos e virtuais.

3. PROTOCOLO DE GERENCIAMENTO DE REDES

3.1. SNMP

O SNMP (*Simple Network Management Protocol* - Protocolo Simples de Gerenciamento de Rede), é um protocolo padrão para monitoramento e gerenciamento de redes. Ele foi desenvolvido para facilitar a gestão de redes, pois permite que produtos e serviços de diferentes fabricantes se comuniquem usando o mesmo protocolo.

> O SNMP é o protocolo de gerência de redes padrão do IETF (Internet Engineering Task Force). Ele é um protocolo pertencente à camada de aplicação do modelo OSI[2] e utiliza na camada de transporte os serviços do protocolo UDP para enviar suas mensagens através da rede. Cada dispositivo gerenciado pode ser definido como Agente.(NOBRE., 2013).

Se baseia no TCP/IP, é totalmente compatível com a Internet. Foi definido nas RFCs 1067 (agosto/1968). e atualmente conta com três versões, SNMPv1 (RFC 1157), SNMPv2 (RFC 1901) estando atualmente na terceira versão, SNMPv3 (RFC 2571). Quase todos os ativos gerenciáveis em uma rede se comunicam via SNMP, sendo usado por muitos serviços como protocolo de gerenciamento.

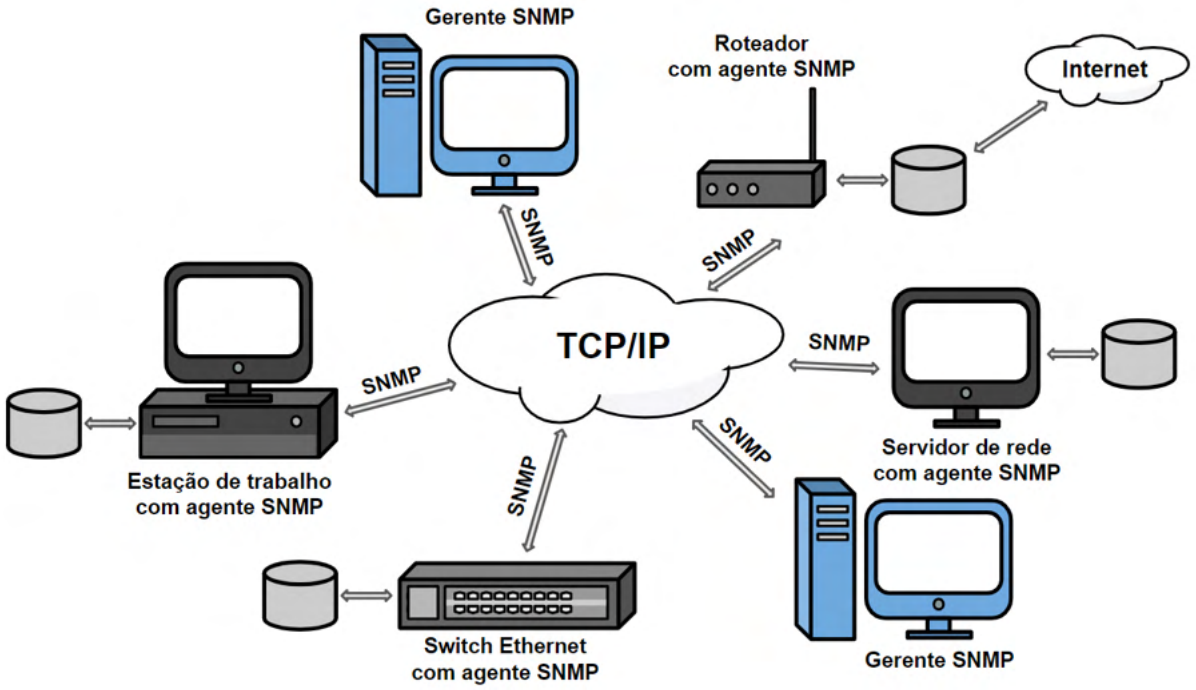
3.1.1. Arquitetura do SNMP

Um protocolo SNMP, faz uso de arquitetura baseada no conceito de agente e gerente, onde o gerente solicita informações do agente, como por exemplo (uso de memória, temperatura, quantidade de endereço IP recebidos e enviados), o gerente realiza a coleta de dados (*pooling*), definindo o formatos e o tipo dos pacotes que serão trocados nessa comunicação.

É um protocolo não orientado à conexão, ou seja, não é necessária nenhuma ação antes ou após o envio da mensagem, com isso não há garantia de que a mensagem chegará até o destinatário. A figura 3 ilustra a estrutura básica do SNMP.

[2] OSI é um modelo de rede de computadores referência ISO dividido em 7 camadas (física, enlace, rede, transporte, sessão, apresentação, aplicação), Ele foi criado para ser o padrão de protocolo de comunicação entre os mais diversos sistemas da rede local, garantindo um sistema de comunicação entre dois computadores.

Figura 3 - Arquitetura do SNMP



Fonte - Adaptado de ROCHA, 2017.

Na figura 3, existem diferentes dispositivos, é possível ter mais de um gerente dentro de uma mesma rede, funcionando de forma simultânea, não há problema, pois os agentes SNMP são capazes de responder simultaneamente a diversos gerentes.

3.1.2. Operações do SNMP

Existem três operações comuns no processo de gestão:

- ***Get* (Obter)*:*** Permite que a entidade gerenciadora recupere o valor de dispositivo gerenciado. Essa recuperação de valor pode ser feita de duas formas:
    - ***GetRequest:*** Recupera a primeira informação da lista de informação de objetos;
    - ***GetNextRequest:*** Recupera a próxima informação disponível na lista, a partir da última informação solicitada;
- ***Set* (Definir)*:*** Permite que uma entidade gerenciada defina o valor de um objeto MIB dos dispositivos gerenciados, para cada *SetRequest* realizado por

uma entidade gerenciada, o dispositivo gerenciado responde com *GetResponse*;

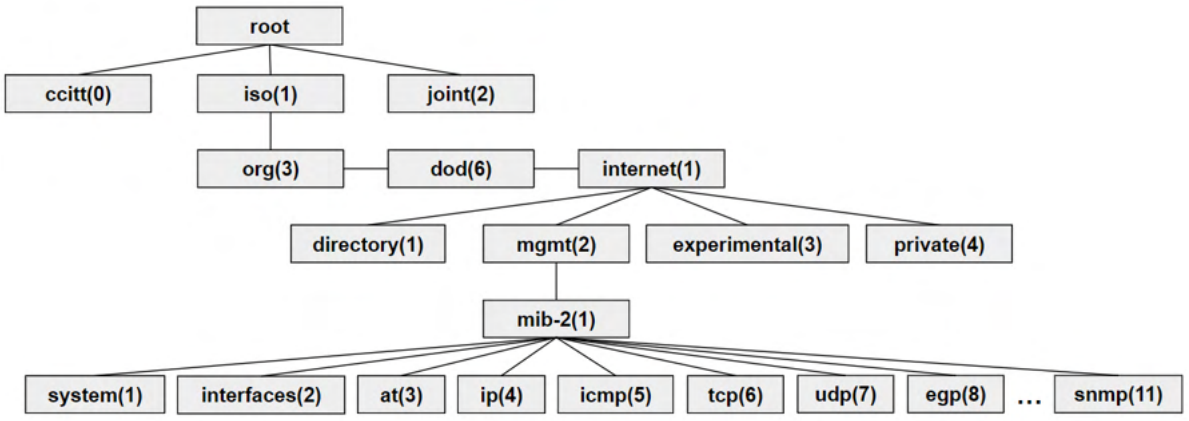
- ***Trap* (Armadilha)*:*** Permitir que dispositivos gerenciados notifiquem entidades gerentes sobre eventos de grande relevância.

3.2. MIB

Na estrutura de gerenciamento padrão da Internet, as informações são representadas como uma coleção de objetos gerenciados. Para Filho (2012) o conjunto de objetos gerenciados com seus respectivos dados dentro de um sistema aberto define a Base de Informações de Gerenciamento ou *Management Information Base* (MIB).

De forma resumida, a MIB funciona como um banco de dados lógico que armazena todas as informações que o agente pode passar ao gerente. Pode-se dizer que a MIB é um mapa que descreve em forma de árvore hierárquica , todos os objetos gerenciados e a forma como eles serão acessados.

Figura 4 - Estrutura da árvore MIB.



Fonte - Adaptado de SILVA, 2018.

Seguindo a árvore representada na Figura 4, As chamadas que usam o protocolo SNMP, podem ser referenciadas aos módulos de interface de duas maneiras.

- Usando os nomes: "iso.org.dod.internet.mgmt.mib-2.ip";
- Usar os números: "1.3.6.1.2.1.4".

4. FERRAMENTAS DE GERENCIAMENTO DE REDES

4.1. As principais ferramentas de gerenciamento de redes

Existem inúmeras ferramentas de monitoramento de redes, sendo elas livres ou pagas. Algumas das mais populares são: Nagios, MRTG, Cacti, NTOP e Zabbix. Também existem softwares que são planejados e desenvolvidos dentro das próprias organizações, visando atender especificamente suas necessidades de monitoramento.

Essas ferramentas possuem a mesma finalidade, mas cada uma tem suas peculiaridades, assim, algumas são mais indicadas para tipos específicos de monitoramento, por isso é importante conhecer bem cada uma dessas *softwares*.

4.1.1. Nagios

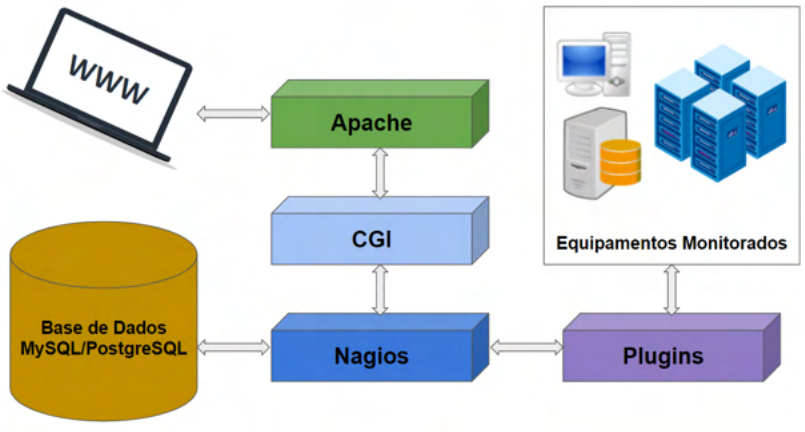
O Nagios[3] é uma ferramenta GPL (*GNU public license*), desenvolvida por Ethan Galstad para o monitoramento da rede. Trata-se de uma ferramenta robusta que possibilita monitorar micros, *switches*, impressoras e todos os demais ativos de TI conectados à rede, verificando constantemente a disponibilidade dos equipamentos, local ou remoto, avisando através de e-mail ou celular o administrador da rede, quando na ocorrência de um problema.

> A eficácia do Nagios no monitoramento de uma rede depende de sua expansão através de plugins, complementos escritos em CGI – *Common Gateway Interface* – ou em qualquer outra linguagem interpretável, podendo ser desenvolvidos por diferentes programadores (ANDRADE, 2008).

O Nagios foi desenvolvido usando como base a arquitetura servidor/agentes, o mesmo é executado em um servidor específico, e seus plugins distribuídos nos servidores que vão ser monitorados, como representado na Figura 5.

[3] https://www.nagios.org/

Figura 5 - Arquitetura do Nagios



Fonte: Autoria Própria.

Como mostra a Figura 5, os plugins enviam informações para o servidor, que é onde o Nagios está instalado, que então exibe essas informações na interface gráfica, esse processo é dividido em 3 partes.

- O *scheduler* faz parte do servidor Nagios. Ele é responsável por verificar os plugins, e executa ações específicas de acordo com os resultados obtidos;
- A interface gráfica do Nagios é exibida em páginas web, geradas pelo *CGI* que exibe as informações como, alertas, configurações e etc. Os dados, podem ser apresentadas na forma de sons, gráficos MRTG e botões de estados:
    - Verde: Normal;
    - Amarelo: Alerta;
    - Vermelho: Erro).
- Os *plugins* são responsáveis por coletar as informações dos servidores e enviar para o Nagios, os mesmo podem ser configurados pelo usuário.

Com o Nagios, pode-se obter relatórios de disponibilidade e configurar ações corretivas para problemas que surgem em sua rede. Sua interface permite monitoramento via WAP e navegador. O software é suportado pelos desenvolvedores e por quem já o utiliza, através de listas de discussão, fóruns online, documentação online e através de FAQs (*Frequently Asked Questions*). Outros recursos fornecidos pelo Nagios incluem:

- Sistemas Operacionais Suportados: Linux e FreeBSD;

- Monitoramento de serviços de rede, como SMTP, POP3, HTTP, NNTP, PING, etc;
- Interface WEB, que possibilita;
    - Verificar o estado corrente da rede;
    - Notificações;
    - Histórico de problemas;
    - Log, etc.
- Monitoração dos recursos dos host (disco, memória, carga do processador, etc);
- Notificação de alarmes via:
    - E-mail;
    - Pager;
    - Outros métodos definidos pelo utilizador (precisa ser desenvolvido/programado).
- Possibilidade de definir tratadores de eventos, para serem corridos durante os serviços ou eventos de host para resolução pró-activa de problemas;
    - Gerência de Falhas;
    - Gerência de Desempenho;
    - Gerência de Contabilização.

4.1.2. MRTG (*Multi Router Traffic Grapher*)

O *MRTG*[4] é uma ferramenta *GPL*, escrita por Tobias Oetiker e muitos colaboradores, para monitorar o tráfego em *links* de rede. Com ele, o usuário obtém informações em tempo real do tráfego da rede.

> É uma ferramenta de monitoração que gera páginas HTML com gráficos de dados coletados a partir de SNMP(Simple Network Management Protocol) ou SCRIPTS externos. É conhecido principalmente pelo seu uso na monitoração de tráfego de rede, mas pode monitorar qualquer coisa desde que o host forneça os dados via SNMP ou script.(LUIZ et. al., 2015).

O MRTG consiste em um script na linguagem Perl que através do protocolo SNMP lê os contadores de tráfego de roteadores, e os apresenta através de gráficos representando o tráfego da rede monitorada. Os gráficos são incluídos nas páginas da Web e podem ser visualizados em qualquer navegador atual, com MRTG. Algumas de suas principais características são:

[4] https://oss.oetiker.ch/mrtg/

- Sistemas operacionais suportados:
    - Plataformas Unix (Linux, FreeBSD, Solaris, etc)
    - Windows (95 ou superior)
- Licenciado sob a GNU GPL;
- Interface do usuário WEB;
- Comunicação com os objetos gerenciados:
    - SNMPv1
    - SNMPv2
- Alguns recursos:
    - Monitora o tráfego em links de rede;
    - Monitora qualquer variável SNMP;
    - Gera páginas HTML contendo imagens representando o tráfego em tempo real;
    - Gera representações visuais do tráfego durante os últimos 7 dias, das últimas 4 semanas e dos últimos 12 meses;
    - Pode monitorar carga do sistema, sessões “logadas”, disponibilidade de modems dentre outros, utilizando programa externo para coleta dos dados.
- O tempo para coleta das informações pode ser definido, caso não seja, por padrão a coleta acontece a cada 5 minutos;
- Envia notificações de alerta;
- Possui algumas ferramentas:
    - CFGMAKER: Responsável por gerar os arquivos de configuração;
    - INDEXMAKER: Gera páginas de índices, quando muitos itens estão sendo monitorados simultaneamente.
- Principais funcionalidades de gerenciamento atendidas:
    - Gerência de desempenho;
    - Gerência de contabilização;
    - Gerência de falhas.

4.1.3. Cacti

O Cacti[5] é um sistema web completo para monitoramento, gera gráficos ao longo do tempo, criando assim um histórico de monitoramento, que fica armazenado e pode ser acessado a qualquer momento através da interface *Web* do Cacti.

> É uma ferramenta freeware que recolhe e exibe informações sobre o estado de uma rede de computadores através de gráficos, sendo um frontend para a ferramenta RRDTool, que armazena todos os dados necessários para criar gráficos e inseri-los em um banco de dados MySQL. Permitindo tanto o monitoramento e gerenciamento de redes simples até redes complexas, com centenas de dispositivos. (MATOS, 2009).

Foi desenvolvido para ser flexível de modo a se adaptar facilmente a diversas necessidades, bem como ser robusto e fácil de usar, o Cacti gerencia vários dados que o SNMP fornece, como: espaço em disco, utilização da CPU, tráfego de rede, temperatura do equipamento, entre outros.

Sua arquitetura possibilita adicionar novas funcionalidades através de plugins, seguem os principais plugins do Cacti:

- Discovery: Busca na rede, todos os dispositivos que não estão sendo monitorados pelo Cacti e informa se o SNMP está habilitado;
- Hostinfo: Permite visualizar informações do host;
- Monitor: Possibilita visualizar o *status Up/Down* dos hosts. Emitirá um alerta toda vez que um *host* for desativado;
- Ntop: Integra a ferramenta Ntop ao Cacti, possibilitando obter estatísticas sobre a rede;
- Realtime: Permite visualizar os gráficos com informações do monitoramento, em tempo real;
- Settings: Possibilita o envio de E-mails;
- Spine: Melhora o desempenho na coleta de dados SNMP*;*
- Syslog: Torna possível armazenar informações do *Syslog* em um banco de dados *MySQL*, o plugin é usado para visualizar e alertar sobre eventos;
- Thold: É um plugin do Módulo *Threshold* criado por Aurelio DeSimone, permite criar qualquer tipo de alerta baseado em gráficos;
- Weathermap: Permite criar mapas da rede, facilitando a visualização do esquema organizacional dos *hosts* dentro da rede.

[5] https://www.cacti.net/

4.1.4. NTOP

O NTOP[6], é um software livre desenvolvido por Luca Deri, para monitoramento e gerenciamento de redes, pode ser usado tanto em sistemas operacionais Unix(Versão completa) quanto Windows(Versão demo, com algumas limitações).

> O Ntop possui métodos capazes de detectar pacotes que estão sendo transmitidos na rede e segmentá-los de acordo com características que possam ser analisadas visando a identificação de certos comportamentos que possam estar sobrecarregando a rede de um modo adverso às políticas de gerenciamento da mesma (HAMMES et. al., 2018).

As análises realizadas pelo NTOP estão mais direcionadas à captura e análise de pacotes e monitoramento de tráfego de rede, O Quadro 1 lista algumas das principais funções dessa ferramenta.

Quadro 1: Funcionalidades do NTOP

Tipo de análise	Descrição
Captura de Pacotes	intercepta os pacotes transmitidos através da rede.
Gravação de tráfego	Monitora em tempo real a taxa de transmissão de dados na rede.
Sonda de Rede	Classificação de tráfego e desvio de pacotes para aceleração.
Análise de Tráfego	Análise de tráfego de alta velocidade baseada na web e coleta de fluxo de pacotes

Fonte: Adaptado de ntop.org.

4.1.5. Zabbix

Entre as diversas ferramentas para gerenciamento de redes, uma das que mais se destaca é o Zabbix[7]. Criado por Alexei Vladishev em 1998 quando trabalhava como administrador de sistemas em um banco, em razão da insatisfação com os sistemas de gerenciamento de rede da época (LIMA, 2014).

O Zabbix é um software de monitoramento de rede projetado para medir a disponibilidade e o desempenho de componentes de infraestrutura, de aplicações e gerar indicadores estratégicos para o negócio. Possui inúmeras vantagens como uma grande quantidade de recursos, facilidade para encontrar documentações e tutoriais relacionados, além de ser uma ferramenta grátis.

[6] https://www.ntop.org/
[7] https://www.zabbix.com/

> O Zabbix promete ser a ferramenta mais completa dentre as GPL, pois une todas as opções que as demais debaixo de uma interface robusta e amigável. Gráficos e mapas são facilmente gerados e acessados e os agentes remotos propiciam um levantamento detalhado do ambiente, ainda que não tenham a mesma qualidade visual de outros produtos (tendência essa seguida por todos os produtos GPL). A documentação excelente facilita a vida do administrador e o software é constantemente atualizado, com comunidade ativa e participante (BLACK, 2008).

Podem-se criar maneiras adicionais para a notificação, possibilitando a integração com ferramentas de terceiros. A representação das informações coletadas são feitas de maneira intuitiva. Para Nunes (2018), “A apresentação dos dados pode ser feita por mapas de rede interativos, gráficos que auxiliam na interpretação das informações captadas e que ainda podem ser integrados em telas de apresentação com características específicas”. Estes mapas e gráficos ajudam o gerente da rede a entender melhor as informações.

O Zabbix oferece soluções para qualquer tipo de infraestrutura de TI, serviços, aplicativos, recursos em nuvem, esse monitoramento é dividido em dois tipos principais: monitoramento de redes e servidores. Os Quadros 2 e 3 mostram algumas das características do monitoramento desses dois tipos de monitoramento.

Quadro 2: Monitoramento de Redes (continua)

Redes		
Desempenho de rede	**Saúde da rede**	**Mudanças na configuração**
Uso de largura de banda da rede	Link desativado	Novo dispositivo adicionado ou removido
Taxa de perda de pacotes	O status do sistema está em estado crítico / de aviso	O módulo de rede é adicionado, removido ou substituído
Interface incorreta	A temperatura do dispositivo está muito alta / muito baixa	O firmware foi atualizado
Alta utilização de CPU ou memória	A fonte de alimentação está em estado crítico	O número de série do dispositivo foi alterado
O número de conexões tcp é anomalia alto para este dia da semana	O espaço livre em disco é baixo	A interface mudou para velocidade mais baixa ou modo half-duplex
O rendimento agregado dos roteadores principais é baixo	O ventilador está em estado crítico	

Fonte: Adaptado de zabbix.com.

Quadro 3: Monitoramento de Servidores

Servidores		
Desempenho do servidor	**Disponibilidade do servidor**	**Mudanças na configuração**
Alta utilização de CPU ou memória	O espaço livre em disco é baixo	Novos componentes adicionados ou removidos
Uso de largura de banda da rede	O status do sistema está em estado crítico / de aviso	O módulo de rede é adicionado, removido ou substituído
Taxa de perda de pacotes	A temperatura do dispositivo está muito alta / muito baixa	O firmware foi atualizado
Taxa de erro da interface	A fonte de alimentação está em estado crítico	O número de série do dispositivo foi alterado
O número de conexões tcp é anomalia alto para este dia da semana	O ventilador está em estado crítico	A interface mudou para velocidade mais baixa ou modo half-duplex
O rendimento agregado dos roteadores principais é baixo	Nenhuma coleta de dados SNMP	

Fonte: Adaptado de zabbix.com.

5. NETWORK OPERATIONS CENTER - NOC

5.1. O que é o Network Operation Center - NOC?

O Network Operations Center - NOC - ou centro de operações de rede, é o local onde se faz uso de softwares específicos, para realizar o monitoramento e gestão dos eventos de TI.

É uma das melhores maneiras de realizar o gerenciamento. Para Cassol (2015) o objetivo do NOC é monitorar a infraestrutura de TI e realizar a gestão de incidentes. Tendo sempre como meta manter o ambiente o mais estável possível.

5.2. Como funciona o NOC?

Através do NOC é possível detectar problemas de maneira proativa, como por exemplo, consumo de recursos, *links* desativados, lentidão, ataques e etc, possibilitando respostas rápidas e precisas contra falhas.

O NOC possui três elementos fundamentais:

- **Ferramentas:** São responsáveis por coletar as informações, para monitoramento da rede;
- **Profissionais:** Tem como principal função, interpretar as informações apresentadas pela ferramenta;
- **Agilidade:** Correção de problemas de maneira rápida, de modo que não criar instabilidade para os usuários.

Dentre as principais atividades do NOC, estão:

- Monitoramento de redes;
- Resposta rápida em caso de falhas;
- Gestão de comunicações (áudio, vídeo, E-mail);
- Desenvolvimento de relatórios (qualidade desempenho e otimização);
- Gerenciamento de atualizações;
- Instalação e atualização de *software/firmware*;
- Gerenciamento de *firewall*;
- Backup e armazenamento;

- *Intrusion Prevention System* ou Sistema de Prevenção de Instrução (IPS), dentre outras ferramentas de segurança;
- Análise de ameaças.

Assim, o objetivo do NOC é fornecer monitoramento contínuo, para manter o ambiente de TI estável e funcionando o tempo todo. Tendo como objetivo inicial, possibilitar o monitoramento de redes, resposta rápida em caso de falha, desenvolvimento de relatórios

5.3. Quais são os benefícios da implementação do NOC?

Com o NOC, os dados gerados pelos ativos de TI podem ser coletados em tempo real, isso permite levantar informações que podem ser usadas para diagnosticar possíveis falhas ou mal funcionamento em serviço e componentes de *hardware e software*.

Isso é possível, pois essas informações são estruturadas e apresentadas na forma de relatórios detalhados, que informam a condição atual da infraestrutura de TI. Na prática, esses relatórios ajudam os gerentes a obter uma compreensão detalhada do sistema e informar onde é necessária mais atenção ou onde são necessárias melhorias. Ajudando a prever possíveis problemas para que possam tomar medidas proativas para otimizar o sistema e corrigir falhas.

Outra vantagem é que além de poder ser organizado fisicamente, o noc também pode oferecer um serviço de gerenciamento em nuvem, reduzindo assim custos com sua implementação.

6. DESENVOLVIMENTO

6.1. Criação do NOC

Durante a revisão bibliográfica, descobriu-se os principais passos para a criação do NOC, que são;

- Conhecer bem a infraestrutura dos ambientes que serão monitorado;
- Escolher a ferramenta de gerenciamento de redes;
- Escolha do local, para implantar a estrutura física do NOC ou o sistema para implementar o monitoramento em nuvem.

Dessa forma, foi elaborado um inventário contendo todos os equipamentos do LORDI, que é o local onde a estrutura física do NOC foi montada a Tabelas 1 apresenta esse inventário de forma resumida.

Tabela 1: Inventário do LORDI

Rede	Nº	Datacenter	Nº	Microinformática	Nº
Roteadores	2	Servidores	12	Notebooks	5
Switches	12			Netbook	1
KVM switch	6			Ipad	1

Fonte: Autoria Própria.

O ambiente do LORDI é bastante diversificado, de início apenas o servidor principal e o *site* do laboratório serão monitorados, mesmo assim o inventário foi fundamental para entender a estrutura física do ambiente onde o NOC será implantado.

6.2. Escolha da ferramenta

Dentre as ferramentas estudadas, a que melhor atendia às necessidades dos laboratórios, foi o Zabbix, por oferecer soluções para diferentes infraestruturas de TI, como serviços, aplicativos e até mesmo recursos em nuvem, além de se adequar bem a ambientes de pequeno, médio e grande porte. O passo seguinte foi selecionar o banco de dados, pois para funcionar o Zabbix precisa estar instalado em um servidor local ou remoto. Para instalar em conjunto com a ferramenta, o banco de dados escolhido foi o Postgresql, por haver muita

documentação e vários tutoriais de instalação da ferramentas em conjunto com esse banco.

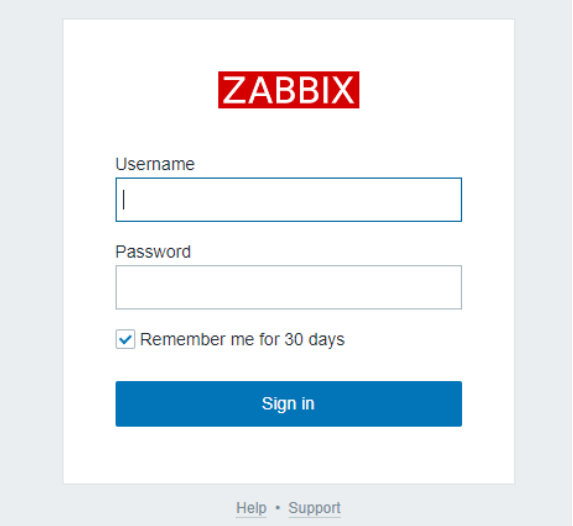
6.3. Instalação e Configurações iniciais do Zabbix

Após realizar uma análise de requisitos, para a instalação e operacionalização do Zabbix, o mesmo foi instalado no Ubuntu server LTS 18.04.2, em conjunto com o postgresql, os passos para instalação da ferramenta foram os seguintes:

- *Download* do pacote no repositório Zabbix;
- Instalação do pacote;
- *Download* dos pacotes necessários para instalação postgresql;
- Instalação postgresql;
- Criação do banco de dados Zabbix no postgresql;
- Configurar o banco (permissões de acesso ao usuário Zabbix);
- Testar comunicação com o banco de dados usuário Zabbix;
- Instalação do Zabbix Server;
- Popular o banco de dados com as tabelas do Zabbix;
- Instalação Frontend;
- Iniciar o Zabbix Server.

Após finalizar o processo de instalação, foi possível acessar a interface *web* do Zabbix, A Figura 6 mostra a tela de login.

Figura 6 - Tela de login na interface web do Zabbix



Fonte: Autoria Própria.

Após a instalação, estudou-se a interface *web* da ferramenta com o objetivo de se familiarizar com a interface, em seguida, usando a documentação disponível em zabbix.com.

Durante o processo de instalação foi desenvolvido uma série de tutoriais, que vão desde a instalação da ferramenta, configurações iniciais dentre outras funções como notificações via E-mail e Telegram, os tutoriais foram desenvolvidos com base em artigos, fóruns e documentação disponível no zabbix.com.

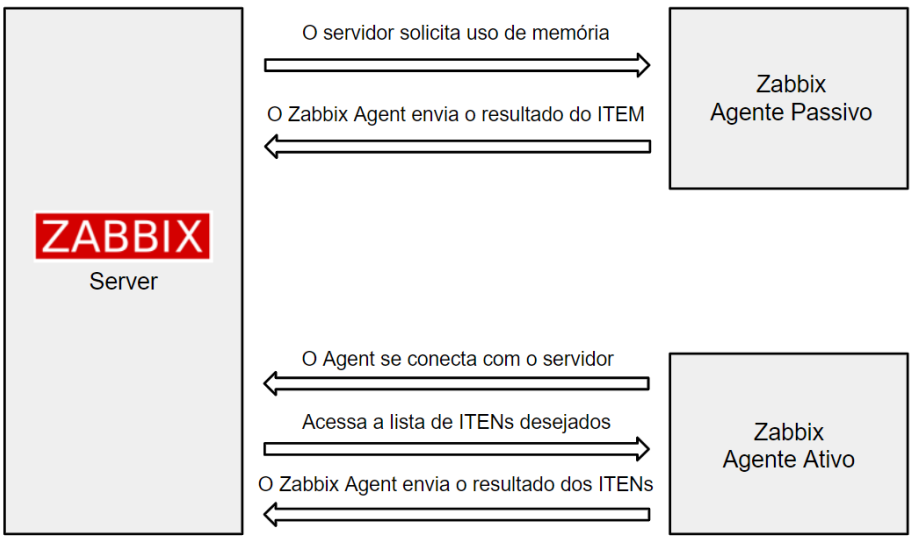
O primeiro passo após a instalação, foi estudar o funcionamento dos agentes no Zabbix. Para Silva (2021) “É uma aplicação instalada no dispositivo a ser gerenciado, que possui capacidade de realizar o monitoramento dos recursos e aplicações como, disco, memória RAM, processador, interface de rede entre outras”,

Existem dois tipos de agentes, passivos e ativos.

> No modo ativo, o agente Zabbix realiza o processamento de forma mais complexa, onde o agente possui uma lista de itens para processamento e o retorno dos valores para o servidor. No modo passivo, o agente apenas responde a uma solicitação de dados do servidor, e envia o resultado da solicitação (ARCENIO., 2015).

A Figura 7, mostra as características de cada tipo de agente.

Figura 7 - Agente ativo x Agente passivo



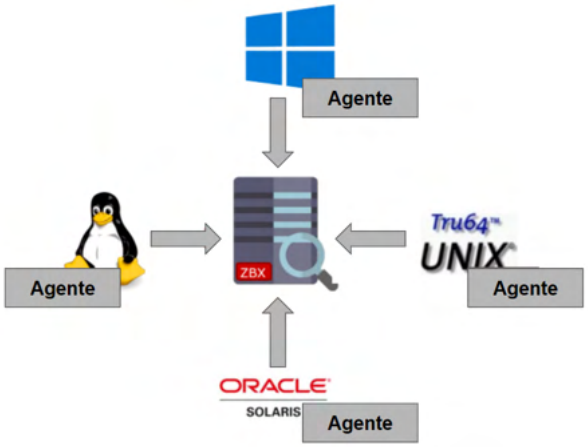
Fonte: Autoria Própria.

A principal diferença entre os dois é a forma de conexão com o servidor, que no caso do agente passivo, o servidor é quem faz as solicitações, já no ativo, o

agente se conecta ao servidor, acessa a lista de itens e devolve os itens de coleta desejados. Neste trabalho, os dois tipos de agentes foram usados.

Os agentes podem ser instalados em diversos *hosts* diferentes, a Figura 8 ilustra um ambiente com ativos diversificados.

8 - Representação do agentes Zabbix em diferentes hosts



Fonte: Adaptado de de SOUZA, 2021.

Em seguida estudou-se os templates, tanto os que já são disponibilizados por padrão como os que podem ser criados para atender necessidades específicas e as triggers. Assim foi possível dar início ao monitoramento do primeiro servidor.

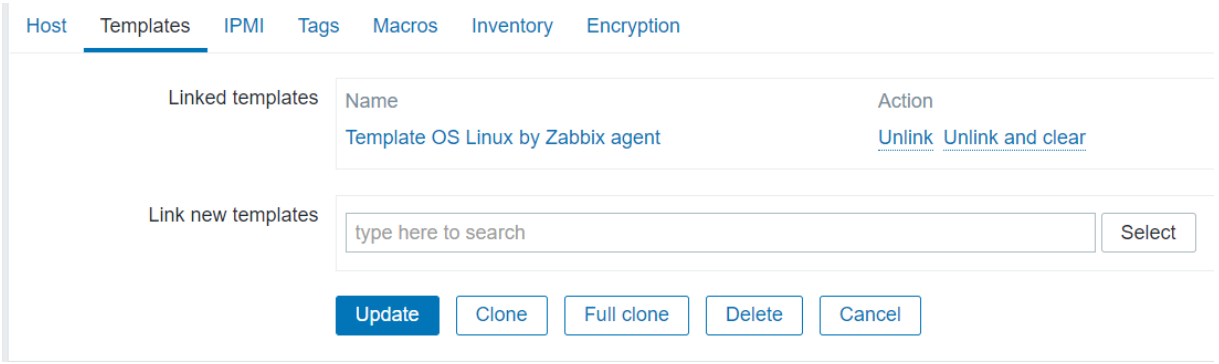
6.3.1. Primeiros passos

O primeiro *host* a ser monitorado foi o do próprio Zabbix, e para isso precisou instalar um agente no servidor, seguindo as seguintes etapas:

- *Download* do pacote no repositório Zabbix;
- Instalação do pacote;
- Abrir arquivo de configurações (vim /etc/zabbix/zabbix_agentd.conf);
    - Dentro do arquivo adicione as informações nos seguintes campos;
      Server: "Ip do servidor zabbix"
      ServerActive: "Ip do servidor zabbix"
      Hostname: "Definir o nome do host"
    - Salvar ("esc + ;" e "wq");
- Startar o agent (*service zabbix-agent start*);
- Verificar se está funcionando (*service zabbix-agent status*).

Para os testes usou-se o *"Template OS Linux by Zabbix agent"*, para usá-lo é preciso ter a versão 5.0 ou superior do Zabbix instalado, não necessitando de nenhuma configuração específica. É preciso instalar o agente Zabbix no sistema operacional Linux que será monitorado, o template faz a coleta de diversas informações essenciais, como espaço em disco, uso de memória, CPU, dentre muitas outras.

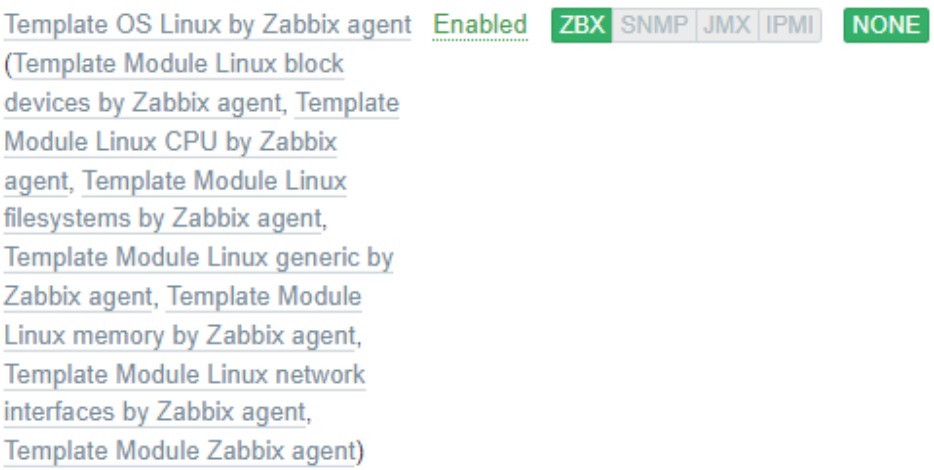
Figura 8 - *Template* usados para monitoramento do primeiro *host*



Fonte: Autoria Própria.

Após a instalação do agente, iniciou-se o monitoramento com sucesso. A Figura 9, mostra os templates ativos no *host*.

Figura 9 - Monitoramento o *"Zabbix Server"*



Fonte: Autoria Própria.

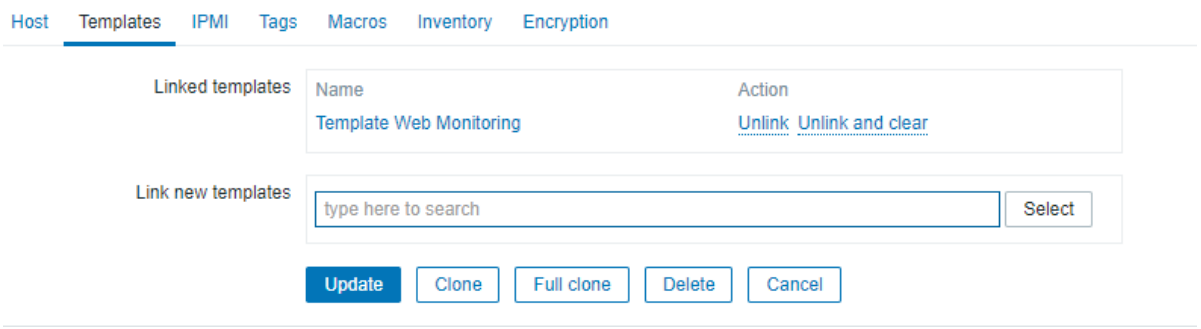
6.3.2. Monitoramento de Sites

Os próximos *hosts* a serem monitorados foram os servidores do Laboratório de Redes e Sistemas Distribuídos - LORDI, Grupo de Engenharia de Software -

GES, e o do Departamento de Informática - DI. Mais especificamente seus *sites*, com o objetivo identificar se a página está online, assim um *template* foi modificado para buscar por uma palavra específicas no corpo do *site*, caso a palavra não seja encontrada, uma mensagem de erro será apresentada, significando que o site provavelmente está *offline. O* "*Template Web Monitoring*" foi modificado e importado para o Zabbix com sucesso.

Após importar o *template*, criou-se um novo *host* chamado "URL LORDI" e o *template* foi adicionado.

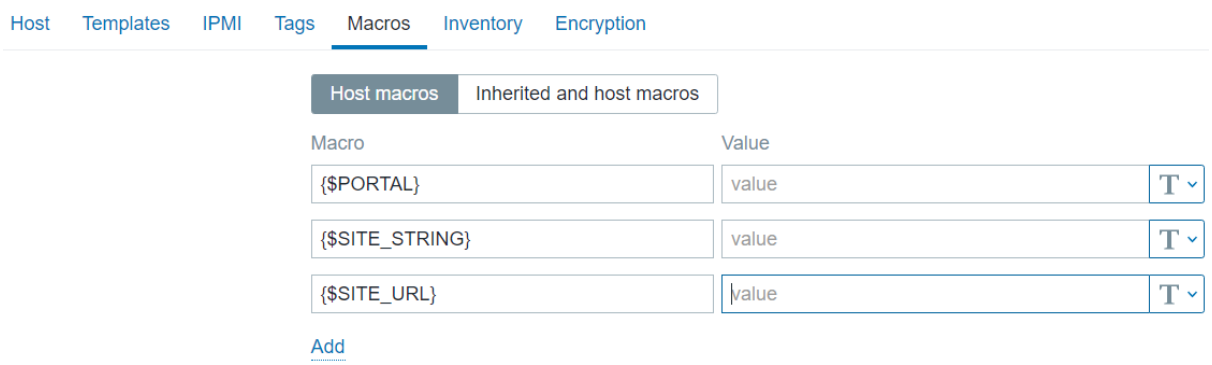
Figura 10 - Adicionando o "*Template Web Monitoring"*



Fonte: Autoria Própria.

Para finalizar, no menu Macros, adicionou-se as informações, como mostrado na Figura 11.

Figura 11 - Adicionando as informações do *site*



Fonte: Autoria Própria.

Em cada campo deve ser adicionado as seguintes informações.

Quadro 4: Descrição dos campos

Campo	Descrição
{$PORTAL}	Nome do portal/*site*
{$SITE_STRING}	Busca uma palavra no corpo da página
{$SITE_URL}	URL a ser monitorado

Fonte: Autoria Própria.

Após verificar que o *template* estava funcionando de forma correta, criou-se os *hosts* do GES e do DI.

Figura 12 - *Hosts* para monitoramento *web* do, LORDI, GES e DI

Fonte: Autoria Própria.

6.3.3. Monitoramento dos *hosts* do LEC

Por fim, foram instalados agentes em quinze dos dezessete computadores do LEC (dois deles apresentaram defeito, por isso não foi possível fazer a instalação), com o objetivo de monitorar e criar um inventário, o LEC é onde se encontra a maior quantidade de *hosts* monitorados, como mostra a Tabela 2.

Tabela 2: Inventário do LEC

hosts	**Nº**	**Sistema Operacional**
Computadores	17	Windows

Fonte: Autoria Própria.

As máquinas são nomeadas usando o seguinte padrão, “LEC-DI-X”, que representa respectivamente:

- LEC: Nome do laboratório;
- DI: Nome do departamento;
- X: Número da máquina, que são numeradas de 1 a 17.

O monitoramento foi feito de forma ativa, por isso o *template* escolhido foi o *"Template OS Windows by Zabbix agent active*", que coleta diversas informações, como, nome da máquina, sistema operacional, uso de memória, entre outros, a Figura 13, mostra alguns dos dados coletados pelo agente.

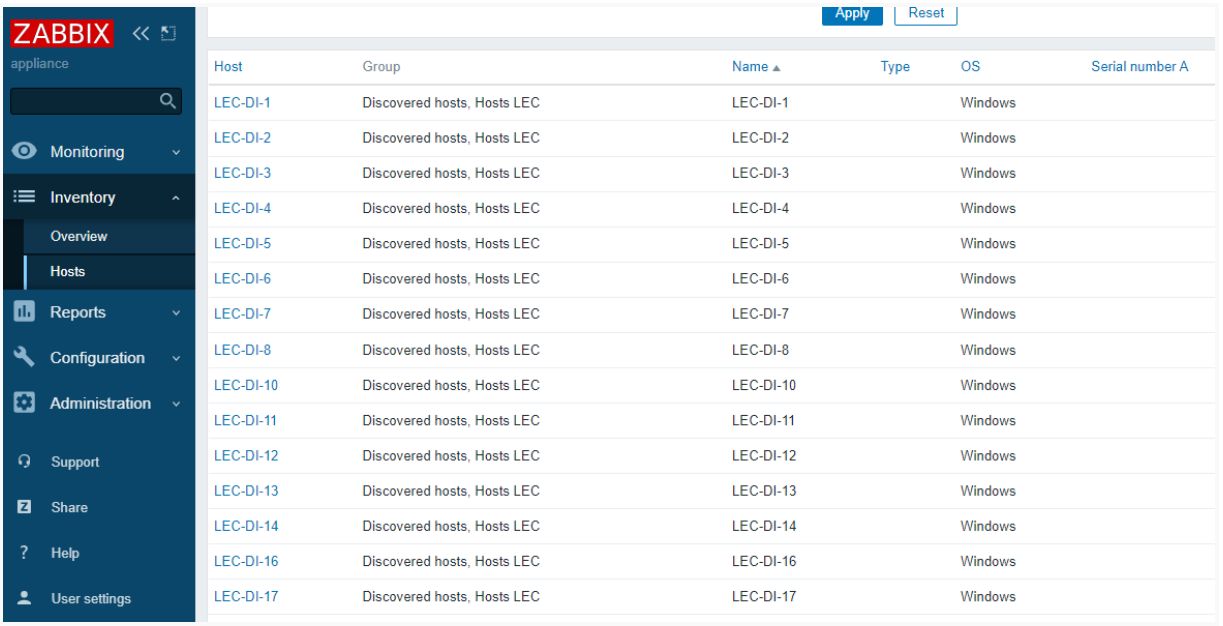
Figura 13 - Informações de coletas do segundo *host.*

General (4 Items)		
System name	2022-04-08 16:24:37	LEC-DI-2
System description	2022-04-08 16:24:37	Windows LEC-DI-2 10.0.1...
Number of threads	2022-04-08 16:24:31	1545
Number of processes	2022-04-08 16:24:36	128
Filesystem C: (3 Items)		
C:: Used space	2022-04-08 16:24:37	61.18 GB
C:: Total space	2022-04-08 16:24:37	118.91 GB
C:: Space utilization	2022-04-08 16:24:37	51.4531 %

Fonte: Autoria Própria.

Também foi possível criar um inventário com todos os *hosts* monitorados do LEC, que pode ser acessado através do menu *Inventory –> Hosts,* como mostra a Figura 14.

Figura 14 - Inventário do laboratório

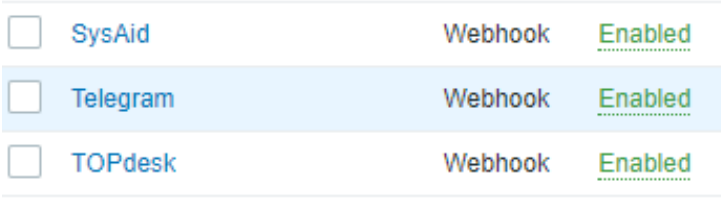


Fonte: Autoria Própria.

6.3.4. Notificações via Telegram

Nas versões anteriores do Zabbix era necessário usar *scripts* ou arquivos disponibilizados por terceiros, para tornar possível as notificações via Telegram, atualmente é possível fazer todas as configurações para essa conexão, diretamente da interface *Web* do Zabbix. Ao acessar o menu *media types,* é possível visualizar todas as opções de mídias disponíveis atualmente.

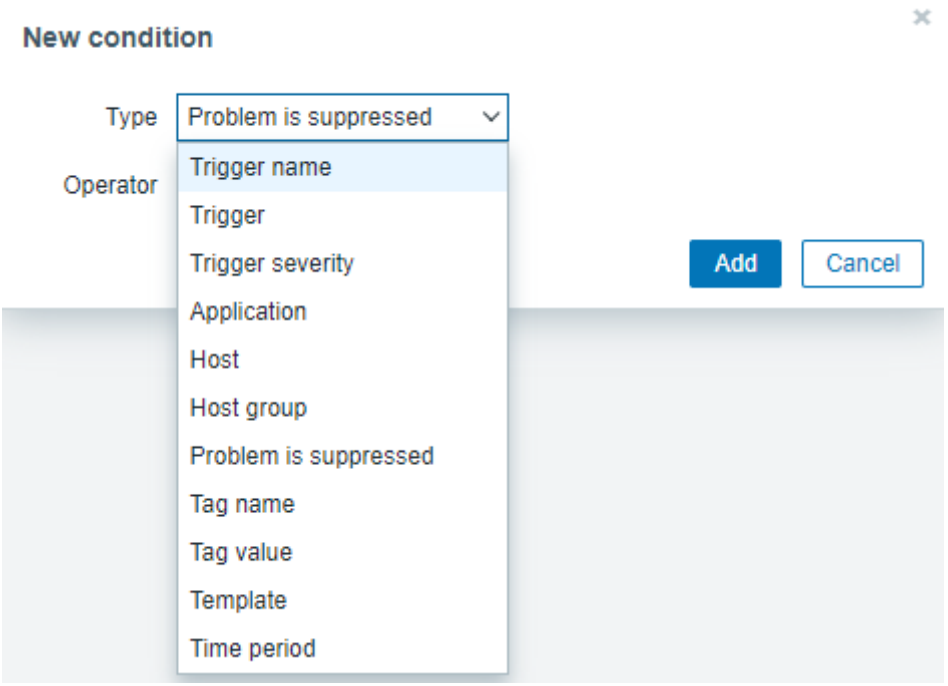
Figura 15 - Telegram listado no menu *media types*



Fonte: Autoria Própria.

Para fazer a conexão, é preciso criar um *bot* e identificar o *token* da conta do Telegram, para qual deseja-se enviar as notificações. Após fazer isso, basta configurar no menu *actions,* as condições para envio da mensagem. A Figura 16 apresenta uma lista com os tipos de ações disponíveis.

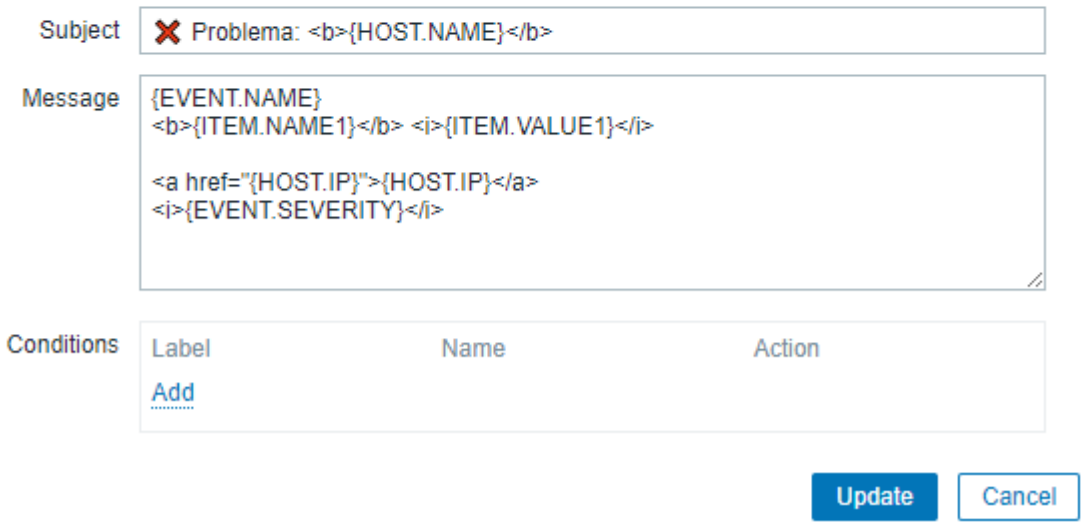
Figura 16 - Tipos de ações



Fonte: Autoria Própria.

No mesmo menu, existe a opção *Operations,* nele se define o formato das mensagens e outros detalhes relacionados ao envio.

Figura 17 - Definindo mensagem



Fonte: Autoria Própria.

Ao finalizar, as mensagens passaram a ser enviadas para o *bot,* como mostra a Figura 18.

Figura 18 - Teste e primeira notificação

Fonte: Autoria Própria.

O Telegram se torna uma ótima opção para o envio das notificações, pois além de estar disponível nos dispositivos móveis, também pode ser acessado pelo computador. O tutorial com todos os detalhes para a conexão e configurações se encontram no “APÊNDICE B - Notificações Via Telegram”.

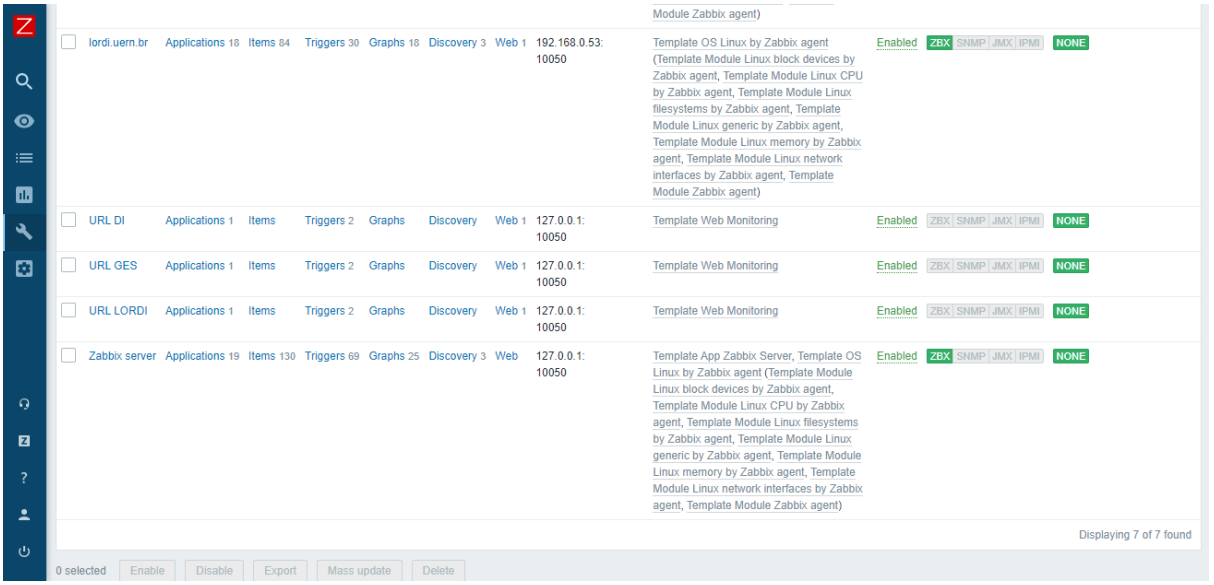
7. RESULTADOS

O presente estudo, permitiu identificar o *software* de gestão Zabbix, como o mais adequado para o gerenciamento da rede dos laboratórios do departamento de informática. A instalação e configuração da ferramenta foi relativamente simples, tendo em vista que existem diversos tutoriais disponibilizados pela comunidade, que podem ser encontrados em fóruns, grupos e páginas da internet, além disso, o próprio site oficial do Zabbix disponibiliza uma documentação bastante completa, o que facilita muito para quem está iniciando com a ferramenta.

Durante o desenvolvimento do projeto foram criados diversos tutoriais, visando deixá-los mais didáticos e facilitar o acesso, os mesmos ensinam desde a instalação e configuração iniciais até a criação e configuração dos agentes, todos os tutoriais criados estão armazenados em um repositório do GitHub.

Atualmente o Zabbix monitora 15 *hosts* no LEC, os servidores do DI, LORDI e LES, e seus respectivos sítios eletrônicos, a Figura 19 mostra alguns dos principais *hosts* monitorados.

Figura 19 - Tela de *hosts* monitorados

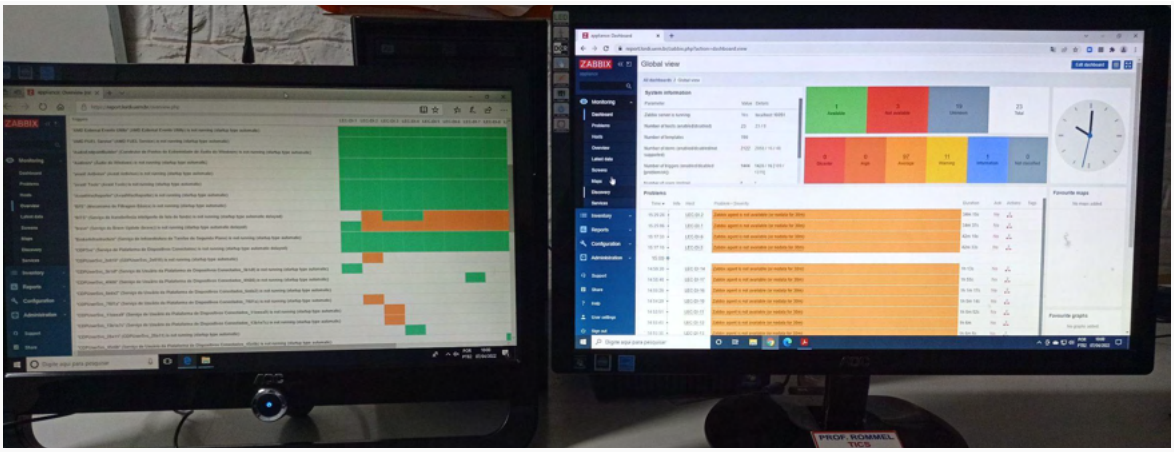


Fonte: Autoria Própria.

O sistema está implementado em nuvem, as informações podem ser acessadas a partir de qualquer computador do LORDI, a Figura 20 mostra a

interface, acessada a partir do laboratório.

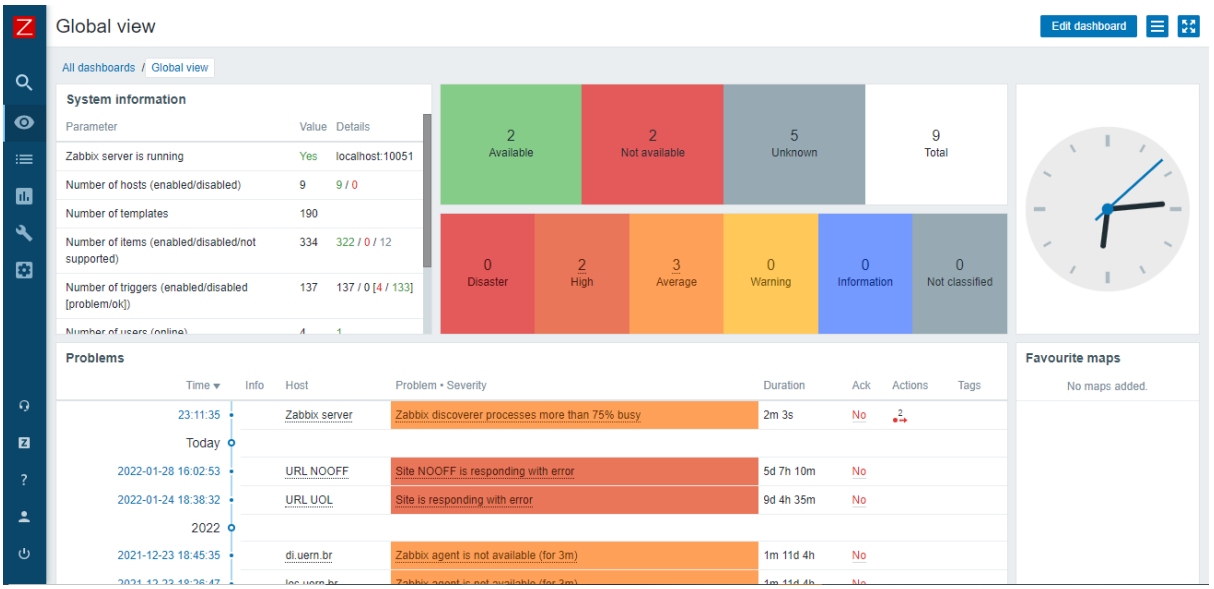
Figura 20 - Estrutura do NOC



Fonte: Autoria Própria.

As informações são apresentadas na tela inicial. A Figura 21 mostra a tela da interface web do Zabbix, onde são apresentadas algumas informações gerais e problemas recentes.

Figura 21 - Notificações na interface *Web* do Zabbix



Fonte: Autoria Própria.

Todos os dados coletados, são enviados ao Telegram em tempo real, fazendo com que essas informações sejam rapidamente acessadas, isso permite uma reação rápida em caso de falha.

7.1. Considerações finais

No desenvolvimento deste trabalho, pode-se perceber a importância do monitoramento de equipamentos e serviços que são prestados através das redes de computadores. Durante esse período, foi possível acompanhar diversas ocorrências de falhas, indisponibilidade, dentre outros problemas em equipamentos, serviços e sistemas.

O acesso rápido às informações de gerenciamento, permite aos administradores do NOC, tomar decisões rápidas e consistentes para garantir a disponibilidade e a prevenção de erros, dos ativos de TI no ambiente monitorado.

Com a implantação do NOC no LORDI, através da ferramenta de monitoramento e gerenciamento de redes de computadores Zabbix pode-se listar alguns dos principais recursos e benefícios.

Relacionado aos pontos positivos da implantação do Zabbix, o sistema é totalmente gratuito e regido pela licença GPL, ou seja, para a UERN que depende de recursos públicos, se torna importante reduzir os gastos.

Outro ponto positivo, é que quando iniciou-se o projeto, o DI não possuía nenhuma ferramenta de monitoramento de redes implementada. O presente trabalho tornou possível, monitorar qualquer equipamento dentro do departamento, com a simples instalação de um agente, possibilitando assim, manter o bom funcionamento dos equipamentos que compõem a rede dos laboratórios.

Por fim, outro ponto positivo que merece destaque, está relacionado a comunidade do Zabbix, que é bastante ativa em, fóruns, redes sociais e blogs, se tornando bastante fácil, tirar dúvidas, receber dicas e ajuda *online*.

7.2. Dificuldades encontradas

Durante o desenvolvimento do projeto, encontrou-se algumas dificuldades, não somente com a ferramenta, mas também pela falta de alguns conhecimentos em redes de computadores, que eram essenciais para o desenvolvimento do projeto.

Outro problema foi a curva de aprendizado do Zabbix, que de início pareceu muito complexo, por possuir muitas funcionalidades, que demandam bastante tempo para serem compreendidas.

A maior dificuldade de todas, sem dúvida foi o início da pandemia, o projeto estava sendo desenvolvido de forma presencial a quase um ano, quando as aulas foram interrompidas, o trabalho teve de ser repensado, para ser possível continuar remotamente, isso atrasou bastante, tendo em vista que o servidor funcionava apenas localmente, e a estrutura física do NOC, tinha que ser organizada.

7.3. Trabalhos futuros

Alguns possíveis trabalhos futuros são:

- Para otimizar ainda mais o escopo do monitoramento. Um exemplo é o Grafana que é uma solução de código aberto que permite escrever plugins para integrar com muitas fontes de dados diferentes, essa ferramenta permite, analisar e monitorar dados ao longo de um período de tempo, mantendo assim um histórico de monitoramento, além disso, os dados são mantidos de forma organizada, facilitando o acesso e a compreensão das informações exibidas;
- Automatização de algumas funcionalidades, como, instalação e configuração de agentes, cadastro de *hosts,* detecção automática de *hosts,* entre outros;
- Expandir a quantidade de *hosts* monitorados, podendo expandir para mais departamentos;

REFERÊNCIAS

ANDRADE, Hetty Alves de. Nagios como Solução de Monitoramento de Rede. 2006. Monografia–Curso de Pós Graduação Latu Sensu em Administração de Redes Linux-Universidade Federal de Lavras, Minas Gerais Brasil. Disponível em: http://www. ginux. ufla. br/files/mono-HettyAndrade. pdf-Acessado em, v. 23, 2014.

ARCENIO, Luiz Fernando Stopa. Monitoramento de dispositivos de redes com Zabbix: suas formas de coleta de informações e o custo de armazenamento. Disponível em: http://www.viiiwticifes.ufba.br/modulos/submissao/Upload-215/55153.pdf. Acesso em: 05 abr. 2022.

BLACK, Tomas Lovis. Comparação de ferramentas de gerenciamento de redes. 2008. 64 f. Tese (Doutorado) - Curso de Especialização em Tecnologia, Gerência e Segurança de Redes de Computadores, Ufrgs, Rio Grande do Sul, 2008. Disponível em: https://www.lume.ufrgs.br/handle/10183/15986. Acesso em: 26 mar. 2020.

B. Wijnen, D. Harrington, R. Presuhn (1999) “RFC 2571 — Uma arquitetura para descrever estruturas de gerenciamento SNMP”.

CASSOL, Luciano A.; SPERONI, Eduardo; DALLAPORTA, Lucimara. Implantação do Núcleo de Operação e Controle-NOC na UFSM. 2015.

FLOWTI. Entenda o que é NOC e conheça os benefícios da sua implementação! Disponível em: https://flowti.com.br/blog/entenda-o-que-e-noc-e-conheca-os-beneficios-da-sua-implementacao. Acesso em: 09 mar. 2022.

HAMMES, Anderson Escobar; SCHULTE, Rafael; HORNER, Marcos Pachola. GERENCIADOR DE REDE NTOP. Disponível em: http://docplayer.com.br/49908654-Gerenciador-de-rede-ntop.html. Acesso em: 13 dez. 2021.

INTERNATIONALIT. NOC: O que é um Centro de Operações de Rede? Disponível em: https://www.internationalit.com/post/noc-o-que-%C3%A9-um-centro-de-opera%C3%A7%C3%B5es-de-rede. Acesso em: 09 mar. 2022.

J Caso, M. Fedor, M.L. Schoffstall, J. Davin (1988) “RFC 1067 — Protocolo Simples de Gerenciamento de Rede”.

J. Caso, M. Fedor, M. Schoffstall, J. Davin (1990) “RFC 1157 - A Simple Network Management Protocol (SNMP)”.

J. Caso, M. Keith, R. Marshall, W. Steven (1996) “RFC 1901 — Introduction to Community-based SNMPv2”.

KUROSE, James F.; ROSS, Keith W.; ZUCCHI, Wagner Luiz. Redes de Computadores e a Internet: uma abordagem top-down. Pearson Addison Wesley, Brasil, 2007.

LIMA, Janssen Dos Reis. Monitoramento de Redes com ZABBIX. Rio de Janeiro: Brasport, 2014.

LUIZ, Mateus Matias; RODRIGUES, Edu; ROCHA, Higor; HENRIQUE, Luis. MRTG Multi Router Traffic Grapher. Disponível em: https://docplayer.com.br/2392497-Mrtg-multi-router-traffic-grapher.html. Acesso em: 18 fev. 2022.

MATOS, Leonardo Kolisnik. Gerenciamento de equipamentos de rede utilizando o software CACTI. 2009.

NOBRE, André. Características e Funcionamento do Protocolo SNMP. Sinop, Mt: Slide, 2013. 28 slides, color. Disponível em: <https://pt.slideshare.net/andredrops/protocolo-snmp-28014668>. Acesso em: 03 out. 2019.

NUNES, Luís Antônio. O uso do Zabbix no monitoramento de infraestrutura dos clouds e servidores de uma empresa de software. 2018. 23 f Unisul Virtual, 2020.

PINHEIRO, José Mauricio dos Santos. Conceitos Básicos de Gerenciamento de Redes. Disponível em: https://www.projetoderedes.com.br/tutoriais/tutorial_conceitos_gerenciamento_01.php. Acesso em: 18 fev. 2022.

POLETO FILHO, Olavo. Gerenciamento e Monitoramento de Redes I: Análise de Desempenho. Disponível em: https://www.teleco.com.br/tutoriais/tutorialgmredes1/default.asp. Acesso em: 18 fev. 2022.

SILVA, Paulo Henrick Martins. Gerenciamento de Redes com Zabbix. 2021.

SILVA, R. S. S. Simple Network Managent Protocol (SNMP). Disponível em https://www.gta.ufrj.br/grad/04_1/snmp/index.htm. Acesso em fevereiro de 2022.

SOUZA, DAVI MACHADO; HANNA, MAICON WARTHMANN; ACOSTA, ROBERTO BARTZEN. GERENCIAMENTO E MONITORAMENTO DE REDES COM ZABBIX. REVISTA ACADÊMICA ALCIDES MAYA, v. 2, n. 2, 2020.

SOUZA, Erique. Instalando o Zabbix-Agent no Linux Ubuntu, Debian e CentOS. Disponível em: https://relatosti.com.br/2021/03/instalando-o-zabbix-agent-no-linux-ubuntu-debian-centos/. Acesso em: 19 fev. 2022.

TIINSIDE. Pesquisa aponta 4,66 bilhões de usuários ativos na internet em 2021. Disponível em: Pesquisa aponta 4,66 bilhões de usuários ativos na internet em 2021. Acesso em: 18 fev. 2022.

ZENOSS. Zenoss é reconhecido no Gartner Market Guide para plataformas AIOps. Disponível em: https://www.zenoss.com/. Acesso em: 26 mar. 2020.

APÊNDICES

APÊNDICE A - Download e Instalação do *Template Web Monitoring*

Observações

Antes de iniciar o tutorial, é importante ter o Zabbix instalado e configurado, para isso basta seguir os tutoriais disponibilizados no zabbix.com .

Instalação do Template

O template *Web Monitoring*, monitora sites para verificar se a página está online e retorna outras informações como:

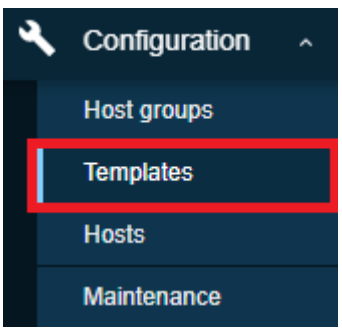
- Tempo de resposta;
- Última mensagem de erro do "Web";
- Falha na etapa do cenário "Web";
- Velocidade de download.

Para instalar o template, siga os passos abaixo.

1. Baixe e Importação:

fazer download do arquivo *"Template Web Monitoring.xml"*, disponível no repositório do GitHub: https://github.com/marcos16165/Tutoriais_Zabbix

Para importar, basta abrir o zabbix, acessar o menu de ***Configuration*** → ***Templates***.



Em seguida, selecione a opção Import na parte superior direita.

Busque o arquivo baixado em seu computador.

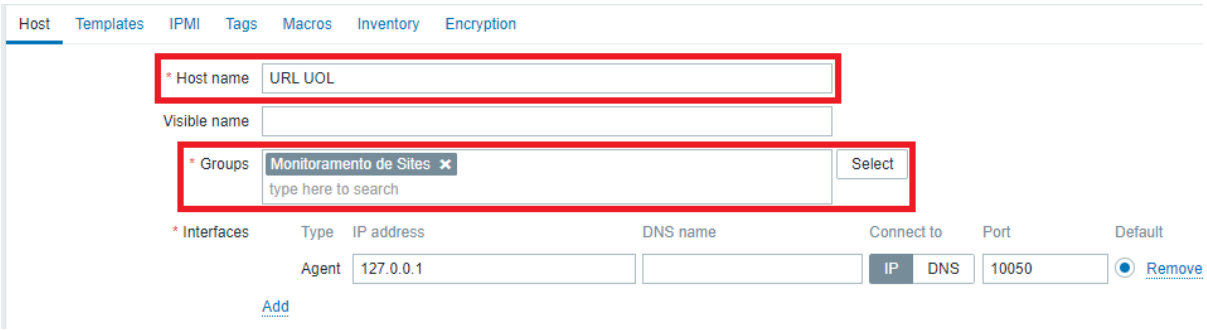
Por fim, selecione a opção Import .

O template foi importado com sucesso.

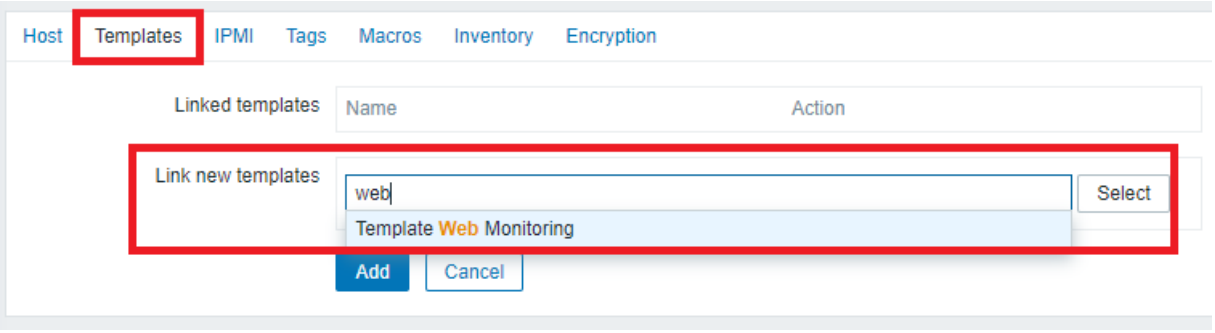
2. Testando o Modelo:

Para testar o template, volte ao menu de ***Configuration*** → ***Hosts***. Na parte superior direita, selecione Create host .

Escolha um nome para o *host*, farei o teste com o site do UOL, por isso nomeei como “URL UOL”, em seguida selecione ou crie um novo grupo.



Selecione o template.

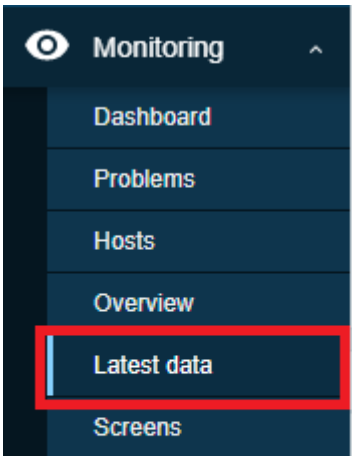


Agora vá até a opção *'Macros*', preencha os campos, selecionando a opção *'Change'*.

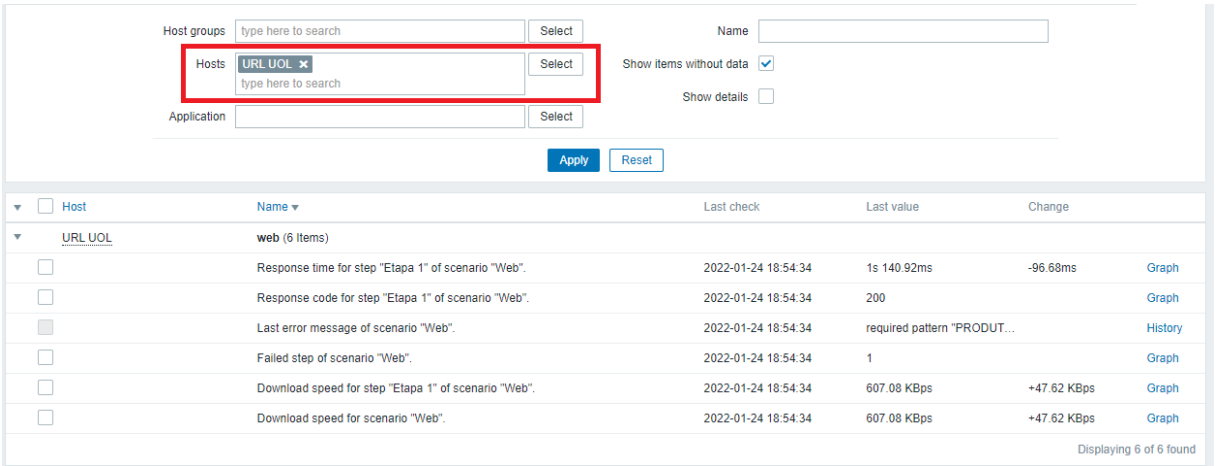
- ***{$PORTAL}:*** Nome do portal/site;

- ***{$SITE_STRING}:*** Busca uma palavra no corpo da página (Exemplo: nome do portal, palavra do cabeçalho e etc. Opte por palavras que estão na página de forma permanente, caso a palavra não seja encontrada, uma mensagem de erro é retornada, indicando que o site está offline);
- ***{$SITE_URL}:*** URL a ser monitorado.

Para verificar se o template está funcionando corretamente, vá até a opção ***Monitoring → Latest data.***



Selecione o *Host*, conforme as informações coletadas serão exibidas na parte de baixo.



APÊNDICE B - Notificações Via Telegram

As versões 5.0 ou superior do Zabbix, possuem o “Telegram/Webhook”, o que torna possível, configurar para enviar alertas via Telegram, sem a necessidade de *softwares* ou *scripts* de terceiros.

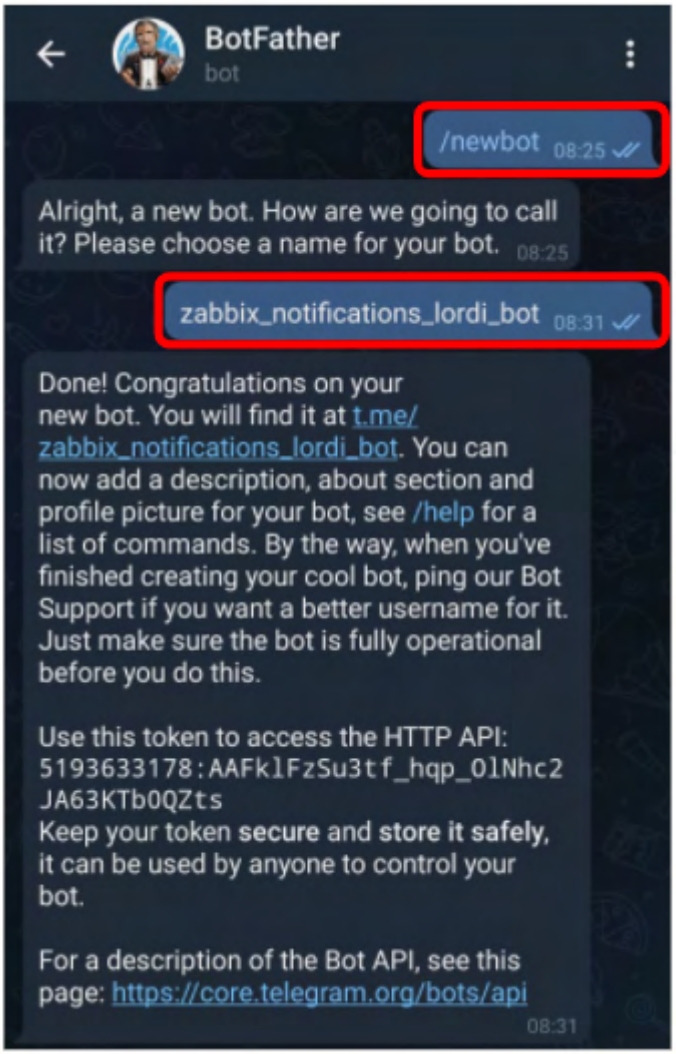
Passo 01: Criando o *bot* no Telegram

Abra o Telegram, e pesquise por ***@BotFather***.

Ao acessar o canal, a seguinte mensagem será exibida.

Para criar o *bot*, digite o comando, no chat ***/newbot***.

Em seguida é só escolher o nome do bot, EX: *“zabbix_notifications_lordi_bot"*



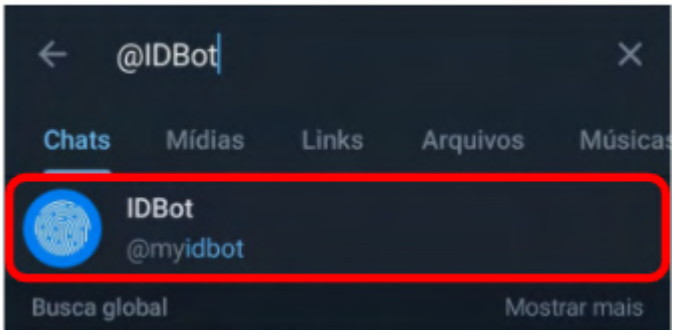
Ao criar o *bot*, uma mensagem com o *token*, será exibida, este *token* será usado nos passos seguintes.

"Use this token to access the HTTP API:"

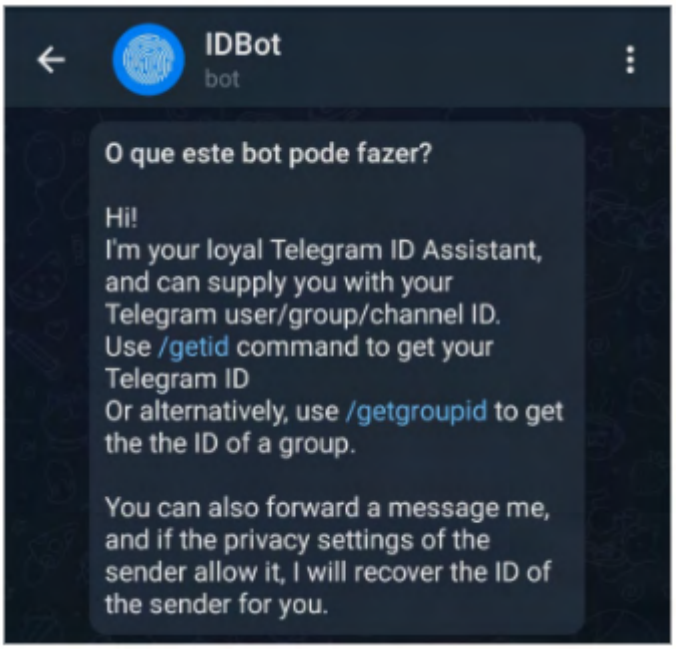
5193633178:AAFklFzSu3tf_hqp_OlNhc2JA63KTb0QZts

Passo 02: Identificando o ID

Abra o Telegram, e pesquise por ***@IDbot***.

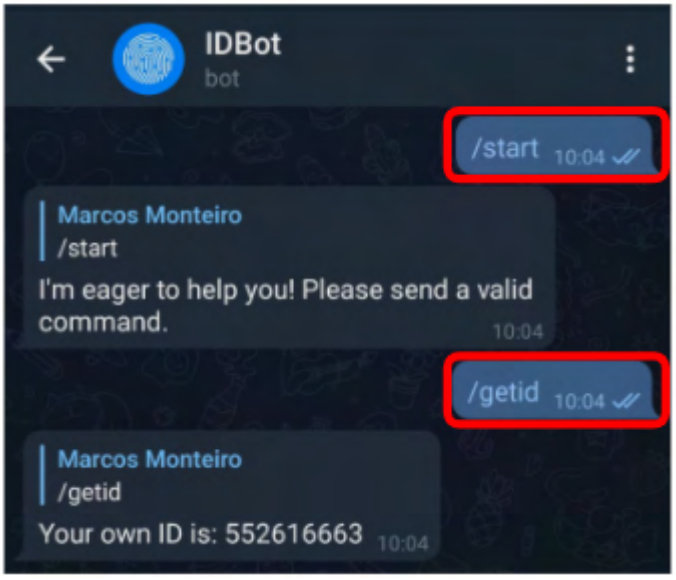


Ao acessar o canal, a seguinte mensagem será exibida.



Para criar o *bot*, digite o comando, no chat ***/start***.

Para descobrir o ID, use o comando ***/getid***.

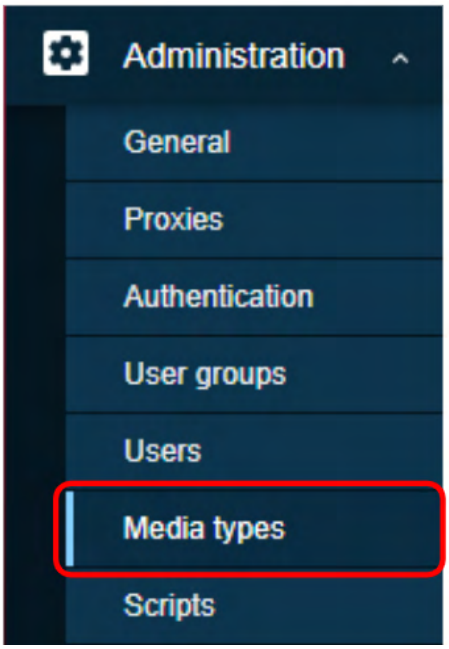


Your own ID is: **552616663**

Guarde o ID, pois ele será necessário para o passo seguinte.

Passo 03: Configurando o Zabbix

Agora acesse ***Administration*** → ***Media types***



Ao acessar o menu, será possível acessar diversos tipos de mídia, localize o Telegram.

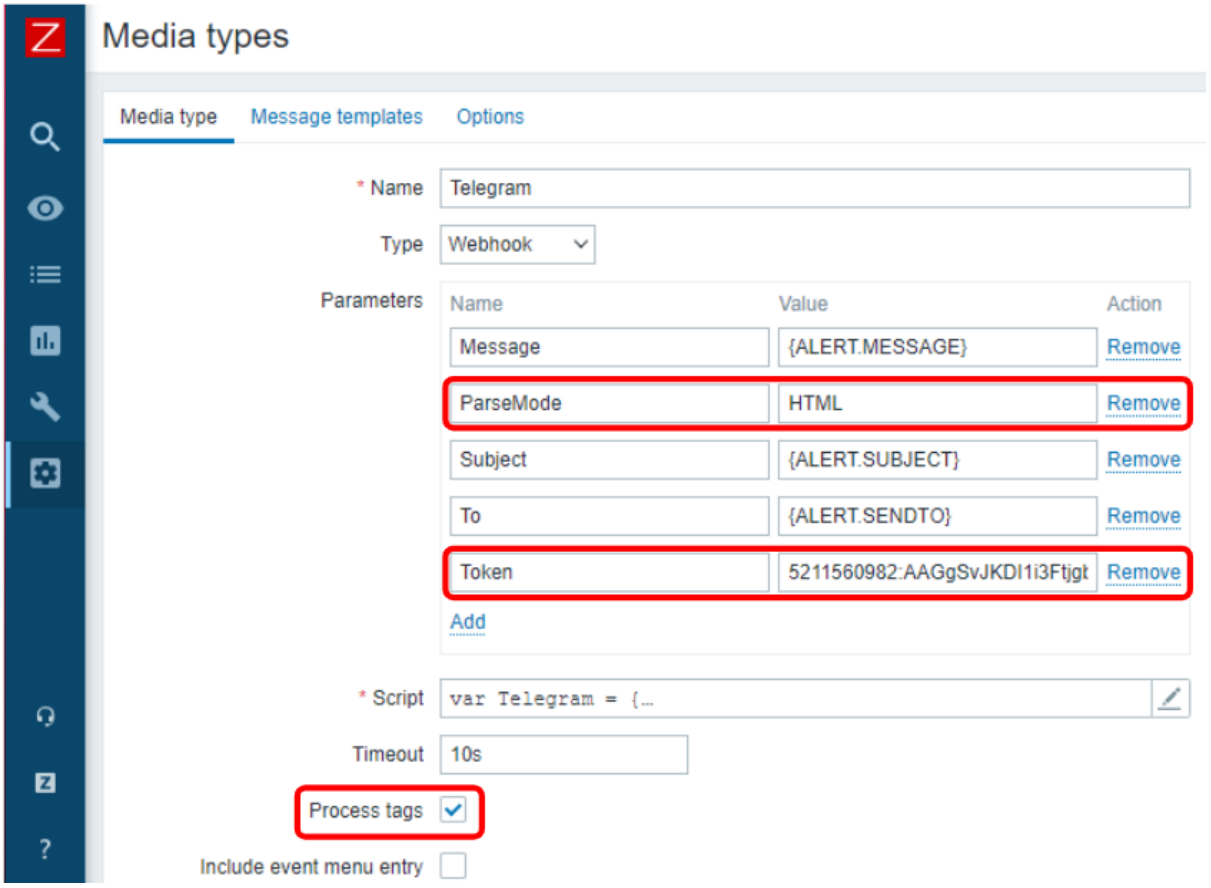
Edite os seguintes campos:

***ParseMode*:** Para HTML;

***Token*:** Adicione o *token* que você criou;

***Process tags*:** Marque a opção.

Ao finalizar vá na parte inferior da página e selecione a opção ***Add.***



Após preencher os campos, é recomendado testar, para saber se as a conexão está funcionando corretamente.

Selecione a opção ***Test***, que está localizada no menu ***Administration*** → ***Media types***, no lado direito da opção Telegram.

Edite os seguintes campos:

Message**:** Adicione uma mensagem;

Subject**:** Adicione uma mensagem;

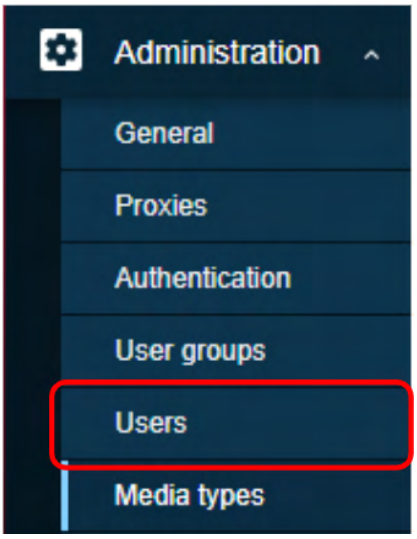
To**:** Adicione seu ID, identificado no segundo passo deste tutorial.

Se tudo estiver funcionando corretamente, você receberá a mensagem no *bot* do Telegram, como no exemplo abaixo.

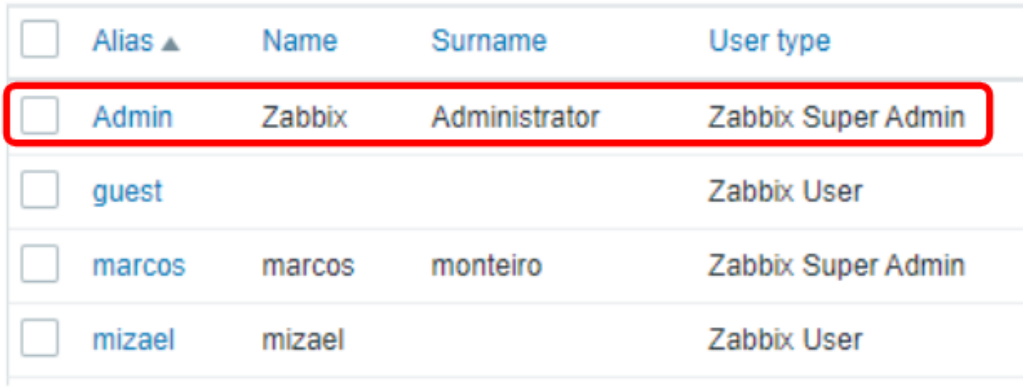
Passo 04: Vinculação com o usuário Zabbix

Com o ID do usuário precisamos vincular ao usuário do Zabbix.

Agora acesse ***Administration*** → ***User***.

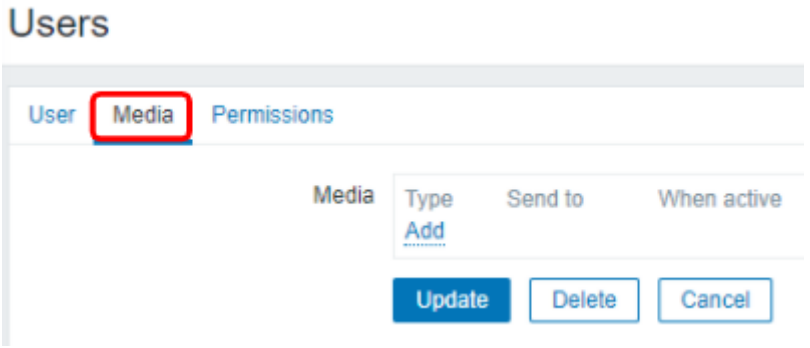


Selecione o usuário, no nosso caso é o Administrador.



Alias ▲	Name	Surname	User type
Admin	Zabbix	Administrator	Zabbix Super Admin
guest			Zabbix User
marcos	marcos	monteiro	Zabbix Super Admin
mizael	mizael		Zabbix User

Ao selecionar o usuário, navegue até ***Media*** e selecione a opção ***Add.***

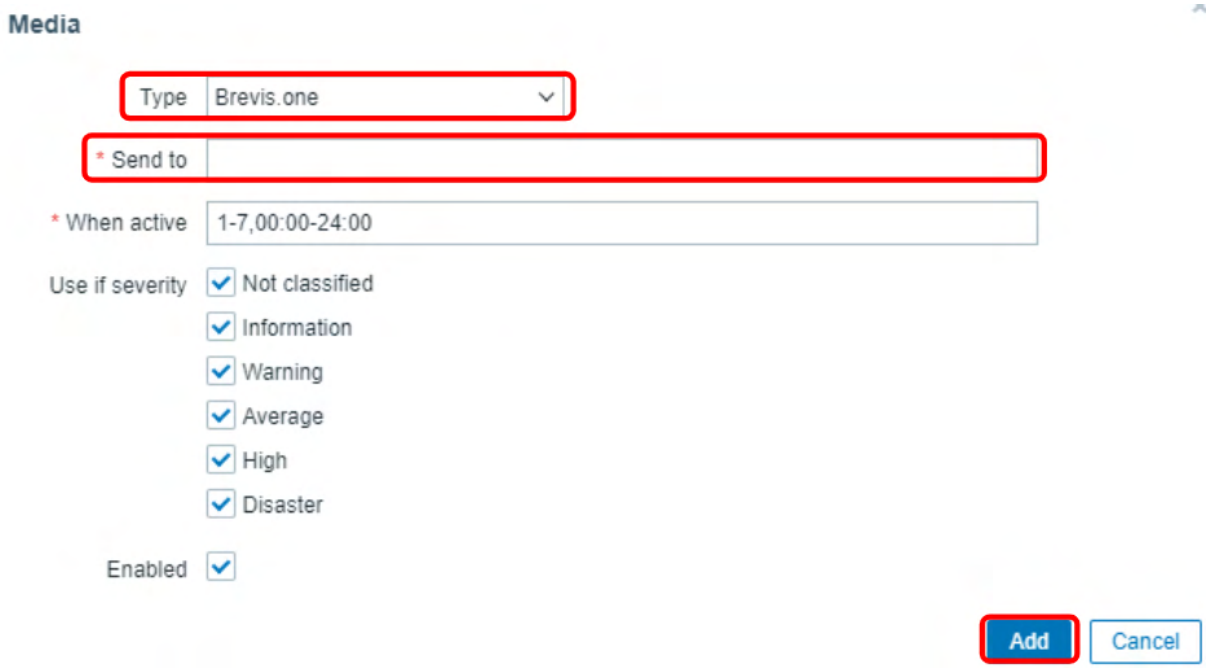


Edite os seguintes campos:

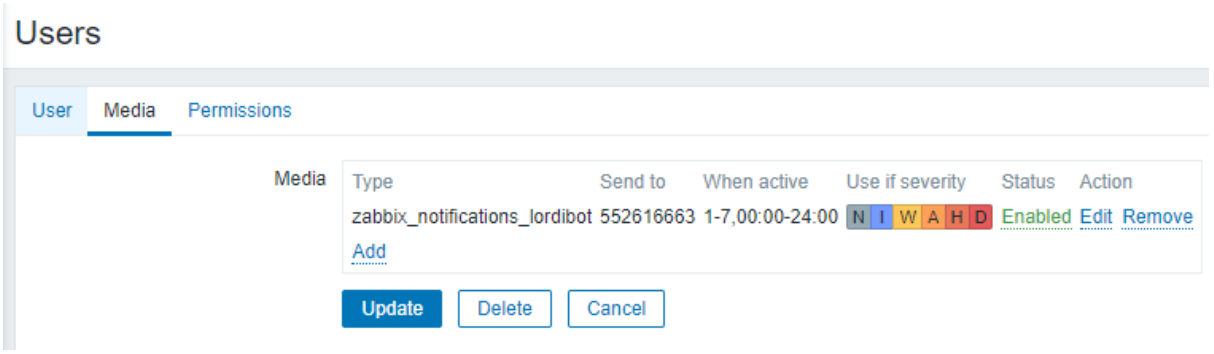
Type**:** Selecione Telegram;

Send to**:** Adicione seu ID;

Clique em ***Add.***

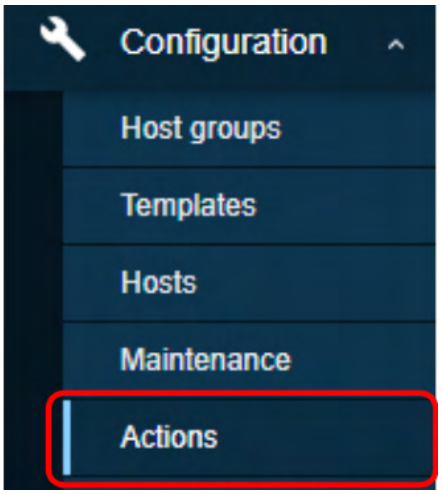


Ao clicar em ***Add***, esse usuário ficará responsável por enviar as notificações.



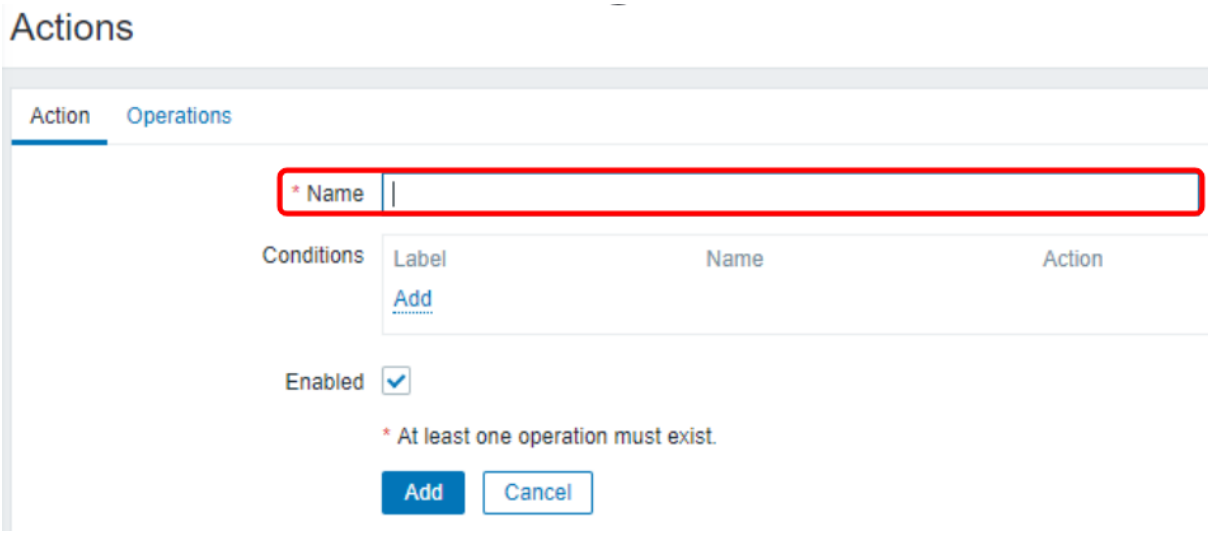
Passo 05: Criando a ação e mensagens para envio dos alertas.

Configuration → Actions

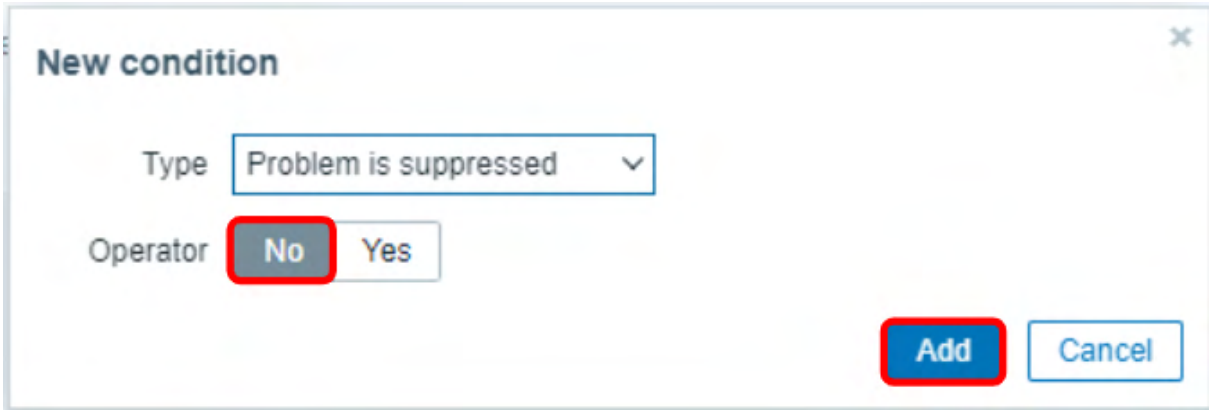


Na parte superior direita, selecione a opção *Create action*

Defina o nome da **Action** e em seguida clique em ***Add.***

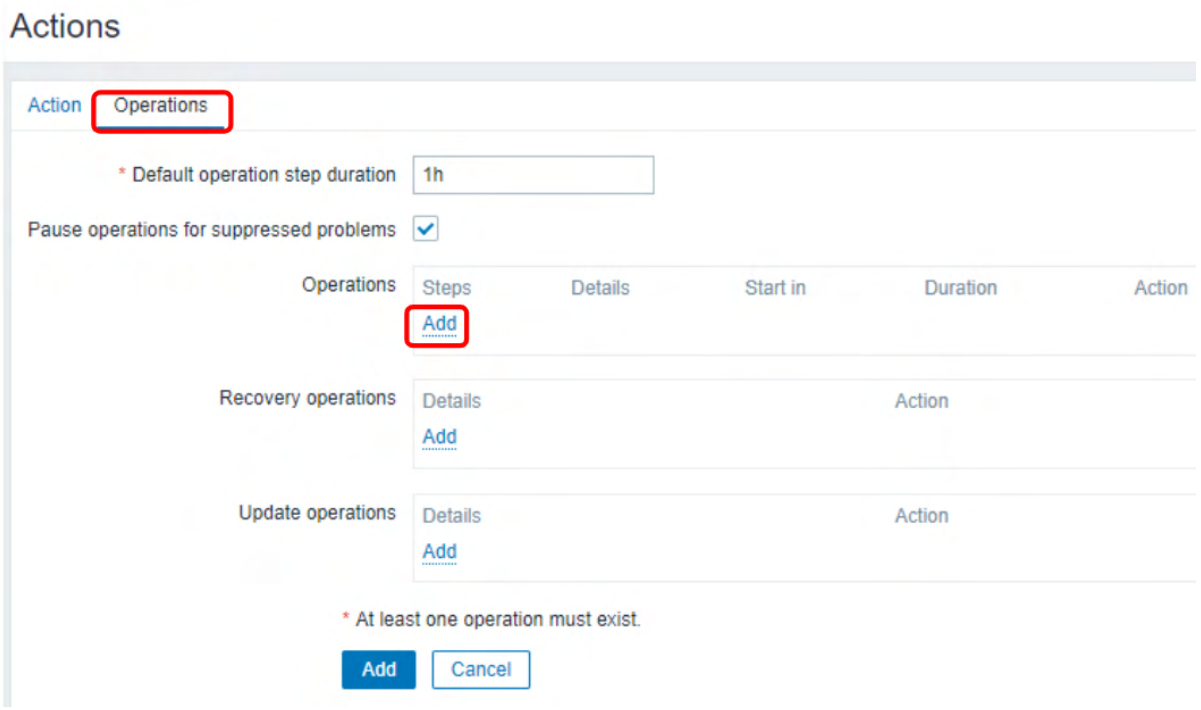


Selecione a opção "*Problem is suppressed"* marquei "*no"* e selecione a opção ***Add.***



Na aba *Operations* vão aparecer três opções: **Operations, *Recovery operations, Update operations.***

Na opção *Operations* selecione ***Add.***



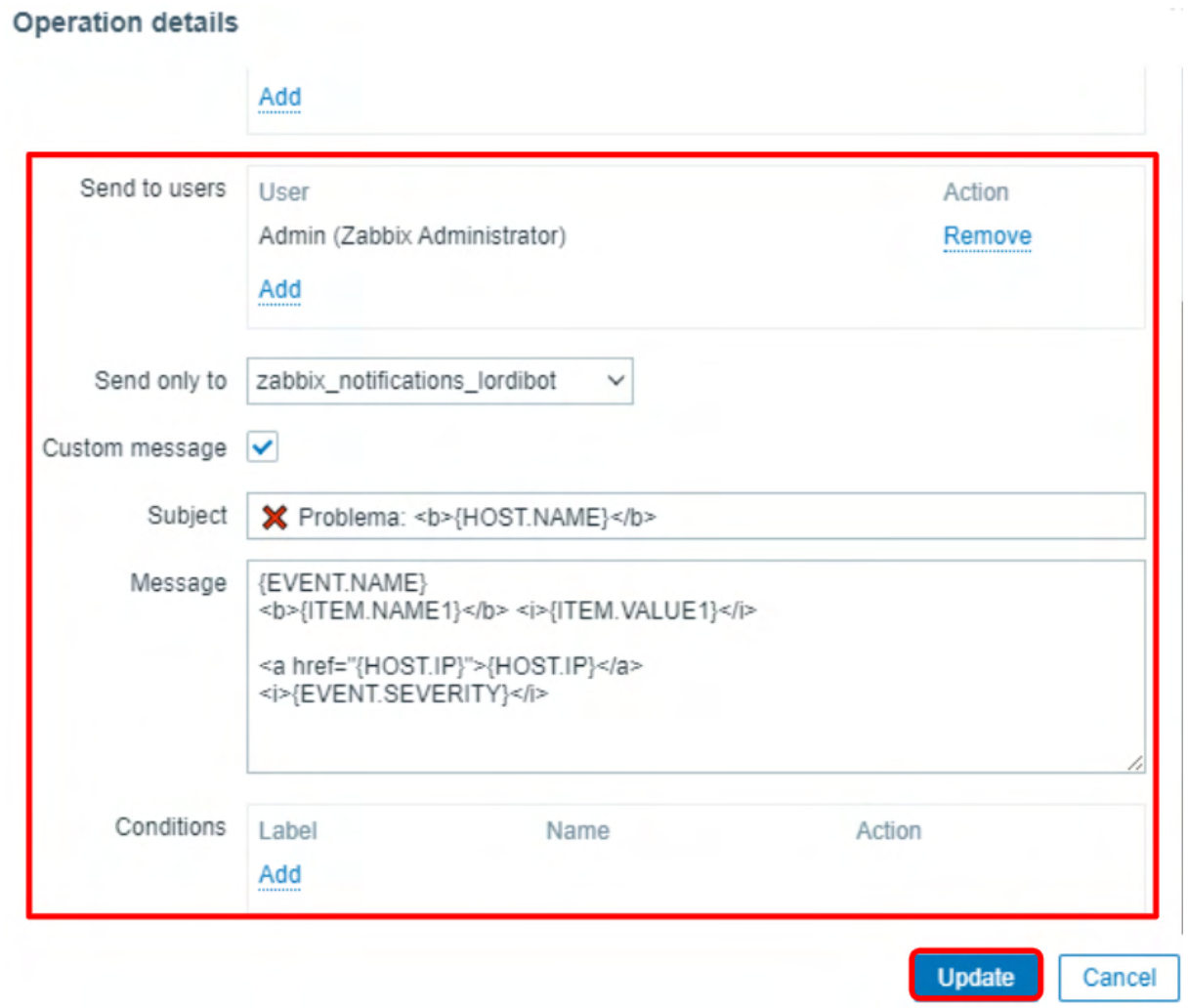
Edite os seguintes campos:

***Send to users*:** Selecione o usuário *Admin*

***Send only to*:** Selecione Telegram caso tenha redefinido o nome, basta selecionar a opção correspondente no meu caso o Telegram está renomeado como "*zabbix_notifications_lordibot*"

Preencha os campos *Subject* e *Message*(O texto se encontra a seguir).

Clique em ***Add.***



O procedimento é o mesmo para as três opções. Mudando apenas a mensagem.

FORMATO DAS MENSAGENS	
Operations	
Subject	❌ Problema: {HOST.NAME}
Message	{EVENT.NAME} {ITEM.NAME1} {ITEM.VALUE1} {HOST.IP} {EVENT.SEVERITY}
Recovery operations	
Subject	✅ Resolvido: {HOST.NAME}
Message	{EVENT.NAME} {ITEM.NAME1} {ITEM.VALUE1} {HOST.IP} {EVENT.SEVERITY}

Update operations	
Subject	Problema atualizado: {EVENT.NAME}
Message	{USER.FULLNAME} {EVENT.UPDATE.ACTION} problema em {EVENT.UPDATE.DATE} {EVENT.UPDATE.TIME}. {EVENT.UPDATE.MESSAGE} O status atual do problema é {EVENT.STATUS}, reconhecido: {EVENT.ACK.STATUS}.

Ao preencher os três, selecione a opção ***Add***, agora as notificações serão enviadas para o Telegram.