MONITORAMENTO DOS RECURSOS DO EQUIPAMENTO RÁDIO L3 HARRIS RF 7800VHH UTILIZANDO O SOFTWARE ZABBIX

Sgt Lucas Pimentel ***Diniz***
Sgt Anderson ***Lucio*** *Gomes*

RESUMO

Este trabalho apresenta uma sugestão de uso do software Zabbix, uma aplicação web open source de monitoramento de ativos de redes, com o foco específico no monitoramento do equipamento rádio L3 Harris 7800V-HH. O Zabbix é uma ferramenta poderosa e versátil que permite às organizações monitorar de forma eficaz seus recursos de rede, garantindo um desempenho otimizado e a detecção precoce de problemas. Neste artigo, exploraremos as funcionalidades essenciais do Zabbix, discutiremos suas vantagens e forneceremos exemplos práticos de sua aplicação no monitoramento do equipamento L3 Harris 7800V-HH que é um ativo crítico em infraestruturas de comunicação.

Palavras-Chave: Monitoramento, Zabbix, L3 Harris 7800V-HH

1. INTRODUÇÃO

Na era da informação e da conectividade ininterrupta, as redes de comunicação desempenham um papel vital em garantir que organizações e instituições possam operar de maneira eficaz e coordenada. A interligação de sistemas, serviços e dispositivos tornou-se uma espinha dorsal para a realização de uma ampla gama de operações críticas, desde comunicações de emergência até missões de defesa e segurança nacional. No centro dessa infraestrutura de comunicação, o equipamento rádio L3 Harris 7800V-HH emerge como um ativo crítico, desempenhando um papel fundamental na manutenção da conectividade e na garantia da eficiência das operações.

A necessidade de monitorar de forma constante e proativa essas redes de comunicação tornou-se inegável. Afinal, a confiabilidade e o desempenho contínuo dessas infraestruturas são cruciais para o sucesso das operações em diversas esferas, desde missões militares até serviços de emergência e comunicações corporativas. O monitoramento não é apenas uma medida preventiva, mas também uma ferramenta indispensável para a identificação precoce de problemas, a manutenção proativa e a melhoria contínua da infraestrutura de comunicação.

No cerne desse contexto, o equipamento rádio L3 Harris 7800V-HH assume um papel de destaque, pois sua capacidade de assegurar comunicações confiáveis em situações desafiadoras o coloca como um componente crítico em infraestruturas de comunicação tática. Seu desempenho e disponibilidade podem afetar diretamente a eficácia das operações, a segurança das equipes e a qualidade dos serviços prestados. Portanto, o monitoramento contínuo desse equipamento é imperativo.

Além disso, o contexto militar e estratégico, juntamente com a gestão eficaz do comando e controle, exige uma compreensão completa da infraestrutura de comunicação e dos ativos associados, como o L3 Harris 7800V-HH. A consciência situacional do comando depende da capacidade de monitorar e responder rapidamente a eventos e problemas que possam afetar a comunicação e, por conseguinte, a capacidade de decisão.

Neste artigo, exploraremos a importância crítica do equipamento rádio L3 Harris 7800V-HH em infraestruturas de comunicação, destacando a necessidade vital de seu monitoramento constante. Além disso, discutiremos como o uso do software Zabbix pode oferecer soluções eficazes para essa tarefa, capacitando organizações a manter operações fluidas, eficientes e seguras em um mundo cada vez mais dependente da conectividade.

2. DESENVOLVIMENTO

2.1 GERENCIAMENTO DE REDES

As redes de computadores modernas são compostas por uma grande variedade de dispositivos que precisam se comunicar e compartilhar recursos. A eficiência dos serviços prestados está associada ao bom desempenho dos sistemas da rede. Para gerenciar esses sistemas e as próprias redes, é necessário um conjunto eficiente de ferramentas de gerenciamento automatizadas.

Com a rápida evolução das tecnologias de redes e a redução dos custos dos recursos compu-

tacionais, as redes de computadores proliferaram em todos os segmentos da sociedade. As redes passaram a fazer parte do cotidiano das pessoas como uma ferramenta que oferece recursos e serviços que permitem uma maior interação entre os usuários e um consequente aumento de produtividade.

O gerenciamento de rede pode ser definido como a coordenação (controle de atividades e monitoração de uso) de recursos materiais (modems, roteadores, etc.) e ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações.

Um sistema de gerência de rede pode ser definido como um conjunto de ferramentas integradas para o monitoramento e controle, que oferece uma interface única e que traz informações sobre o status da rede podendo oferecer ainda um conjunto de comandos que visam executar praticamente todas as atividades de gerenciamento sobre o sistema em questão, PINHEIRO, 2006.

2.2 FERRAMENTAS DE MONITORAMENTO DE REDES UTILIZADAS ATUALMENTE

Há uma grande oferta de aplicações de monitoramento e centralização de logs com ferramentas free e open source:

Zabbix: Esta é uma ferramenta de monitoramento de código aberto que abrange diversos componentes de TI, incluindo redes, servidores, máquinas virtuais e serviços em nuvem. O Zabbix oferece métricas de monitoramento, como uso de rede, carga da CPU e espaço em disco.

Prometheus: Uma ferramenta que coleta informações de aplicativos e infraestrutura, como uso de memória RAM e CPU, e as disponibiliza por meio de um endpoint. Geralmente, é usada em conjunto com outras ferramentas para criar painéis informativos com base nessas informações.

Grafana: Esta ferramenta é usada em conjunto com o Prometheus para criar gráficos e painéis inteligentes que se atualizam em tempo real, permitindo um acompanhamento constante dos dados coletados.

Elastic APM: Similar ao SkyWalking, o Elastic APM possui uma versão de código aberto mais simples que permite a análise em tempo real do tempo de resposta de aplicativos, entre outras funcionalidades.

ELK Stack: O conjunto de ferramentas Beat + ElasticSearch + Kibana é amplamente utilizado para coletar métricas, logs e informações de aplicativos e exibi-los em um painel no Kibana. O ELK Stack é uma solução completa para análise de registros.

Graylog: Com o objetivo de consolidar logs de diversas fontes em um único frontend, o Graylog é usado para gerenciamento, agregação, análise e monitoramento de registros em ambientes que fazem uso intensivo de containers Docker e plataformas de orquestração.

Istio: Essa ferramenta é empregada para monitorar microsserviços em clusters Kubernetes, permitindo a análise das relações entre esses microsserviços e a identificação de possíveis problemas nos sistemas, 4LINUX, 2022.

Snort: O Snort é um sistema de prevenção de intrusões em redes de código aberto, mantido e desenvolvido pela Cisco nos últimos cinco anos. Esta ferramenta se sobressai devido à sua capacidade de analisar o tráfego em tempo real e registrar os pacotes do protocolo TCP (Protocolo de Controle de Transmissão).

Graças a essa versatilidade, o Snort pode cumprir três funções essenciais para monitorar um servidor. Portanto, ele pode ser utilizado como um capturador de pacotes (semelhante ao tcpdump), um registrador de pacotes e/ou um sistema avançado de prevenção de intrusões, DELFINO, 2022.

2.3 A IMPORTÂNCIA DE MONITORAR ATIVOS DE REDE

Estar preparado para ação, ou mesmo agir preventivamente, são resultados de um ambiente de monitoramento eficaz. Além disso, os dados históricos coletados por um sistema de monitoramento competente oferecem insights para a tomada de decisões conscientes sobre aquisições e atualizações de recursos tecnológicos, fundamentadas em análises de capacidade.

Toda essa compreensão do estado do seu sistema é viabilizada por meio de ferramentas de monitoramento que permitem a apresentação visual de métricas por meio de gráficos e mapas. Informações como uso de largura de banda, utilização da CPU, alocação de memória, tempo de consulta do banco de dados e tempo de resposta de solicitações da web podem ser prontamente acessadas, tanto em tempo real quanto em registros históricos.

Um sistema de monitoramento eficiente possibilita a configuração de alertas para eventos anormais e a emissão de notificações com base nesses eventos.

As ferramentas de monitoramento devem garantir que as métricas dos recursos tecnológicos da infraestrutura sejam centralizadas, permitindo que toda a equipe responsável por esses recursos consulte e avalie esses dados. Na maioria das ferramentas de monitoramento, é possível comparar as métricas com valores aceitáveis, facilitando a identificação de irregularidades e, consequentemente, agilizando a resolução de incidentes, quando necessário.

Graças à centralização das métricas, é possível visualizar tendências no uso de recursos de forma gráfica, seja em períodos específicos, como durante o horário comercial ou durante o lançamento de uma nova campanha da organização. O monitoramento inteligente pode ser uma ferramenta valiosa para reduzir os custos relacionados aos recursos tecnológicos, uma vez que a rápida identificação e resolução de incidentes reduzem o tempo de indisponibilidade dos serviços.

2.4 MONITORAMENTO VS DEFESA CIBERNÉTICA

A relação entre o monitoramento de redes e a defesa cibernética é fundamental para garantir a segurança e a eficácia das infraestruturas de tecnologia da informação em organizações. Ambas as áreas desempenham papéis complementares, embora distintos, na proteção contra ameaças cibernéticas. Vamos explorar essa relação em mais detalhes:

O monitoramento de redes envolve a coleta contínua e a análise de dados relacionados ao tráfego de rede, desempenho de sistemas, dispositivos e aplicativos em uma rede, seu objetivo principal é manter a disponibilidade, o desempenho e a integridade da infraestrutura de TI.

Esse monitoramento fornece informações em tempo real sobre a operação da rede, permitindo a identificação de problemas de desempenho, congestionamentos, falhas e problemas operacionais.

A defesa cibernética refere-se a um conjunto de estratégias, políticas, práticas e tecnologias projetadas para proteger sistemas, redes e dados contra ameaças cibernéticas, como ataques de hackers, malwares, phishing e outras atividades maliciosas. O principal objetivo da defesa cibernética é a segurança da informação, garantindo a confidencialidade, integridade e disponibilidade dos dados. Ela envolve a implementação de medidas de segurança, como firewalls, antivírus, detecção de intrusões, autenticação multifator, controle de acesso, criptografia e respostas a incidentes de segurança.

A defesa cibernética é proativa e reativa, visando prevenir ataques, detectar atividades suspeitas e responder a incidentes de segurança quando eles ocorrem.

A Relação entre Monitoramento de Redes e Defesa Cibernética se destaca em:

Detecção de Ameaças:
O monitoramento de redes pode detectar anomalias de tráfego que podem indicar atividades maliciosas. Por exemplo, um aumento súbito no tráfego de saída pode ser um sinal de um ataque de exfiltração de dados. Essas detecções iniciais podem acionar a defesa cibernética para responder rapidamente.

Visibilidade e Contexto:
O monitoramento de redes fornece visibilidade em tempo real da infraestrutura de TI. Essa visibilidade é essencial para a defesa cibernética, pois permite que os profissionais de segurança entendam o contexto em que os eventos de segurança ocorrem e contribui para a consciência situacional.

Resposta a Incidentes:
Quando um incidente de segurança é detectado, a defesa cibernética pode usar as informações coletadas pelo monitoramento de redes para investigar o incidente com mais detalhes e tomar medidas corretivas.

Otimização da Segurança:
O monitoramento de redes também pode ser usado para avaliar a eficácia das medidas de segurança implementadas. Se o monitoramento identificar brechas ou vulnerabilidades, a defesa cibernética pode ser ajustada para reforçar a proteção.

Monitoramento de Ativos Críticos:
A defesa cibernética pode se concentrar em monitorar ativamente sistemas e ativos críticos, enquanto o monitoramento de redes fornece uma visão mais ampla de toda a infraestrutura.

2.5 O EQUIPAMENTO RÁDIO L3 HARRIS 7800V-HH

O dispositivo de comunicação RF-7800V--HH VHF, pertencente à família Falcon III, opera na faixa de frequência entre 30 e 108 MHz, com uma potência variando de 0,5 a 50 Watts quando utilizado em modo veicular. Ao empregar a técnica MELP (Mixed-Excitation Linear Predictive) para codificação e decodificação de áudio, e com uma taxa de transmissão de 2400 bps, ele é capaz de receber sinais fracos que normalmente não seriam captados em comunicações analógicas. Além disso, oferece a capacidade de estabelecer ligações de voz e transferência de dados seguros (COMSEC) por meio de uma rede sem fio que pode ser configurada tanto manualmente quanto por software, possibilitando uma comunicação eficaz em médias de 30 Km para transmissão de voz e 10 Km para transmissão de dados quando usado em veículos.

A integração de uma rede LAN (Local Area Network) na configuração do equipamento permite conectar o rádio a uma rede IP local ou a um dispositivo compatível com esse protocolo, resultando em uma taxa de transmissão de dados IP de 64 kbps em canais com largura de banda de 25kHz e 192 kbps em canais de 75kHz, viabilizando a criação de uma rede de dados simples e a realização de chamadas VoIP simultaneamente à transmissão de áudio, o que é uma característica fundamental desse equipamento.

Ele também dispõe de uma interface USB (Universal Serial Bus) que possibilita o carregamento das configurações do rádio por meio de um pendrive.

2.6 PROTOCOLO SNMP NO EQUIPAMENTO RÁDIO RF 7800V-HH

O SNMP, ou "Simple Network Management Protocol," é o protocolo padrão usado para monitoramento e gerenciamento de redes. Ele é amplamente utilizado para obter informações sobre ativos de rede e serviços. O SNMP permite que um sistema de gerenciamento trabalhe com produtos de diversos fabricantes, tornando-o flexível e interoperável.

No SNMP, os dispositivos gerenciáveis são chamados de "agentes," enquanto os sistemas que consultam ou modificam informações são chamados de "gerentes." O SNMP também permite a geração de alertas (TRAP) em resposta a eventos específicos.

O SNMP é suportado por várias ferramentas de monitoramento de redes, como HP Open View, IBM Tivoli, Nagios e Zabbix. Essas ferramentas podem usar alertas SNMP para notificar os responsáveis sobre problemas.

O SNMP opera com base em um sistema de identificação chamado MIB e OID, que permite ao gerente acessar as informações disponíveis nos agentes. Os OIDs são organizados em uma hierarquia, garantindo a consistência na identificação de dispositivos e serviços.

No contexto do rádio L3 Harris RF-7800V--HH, usado em ambientes militares e de segurança pública, o SNMP é empregado para monitorar e gerenciar aspectos relacionados à rede e ao próprio rádio. Isso inclui:

Gerenciamento de configuração: O SNMP permite configurar o rádio remotamente, facilitando a manutenção em locais com acesso limitado.

Coleta de estatísticas: Pode ser configurado para registrar estatísticas de uso, como chamadas realizadas e uso de frequência, úteis para relatórios e planejamento.

Alarmes e notificações: O SNMP emite alertas em tempo real para identificar e solucionar problemas rapidamente.

Segurança: É importante configurar permissões de acesso adequadas e usar criptografia para proteger as informações transmitidas.

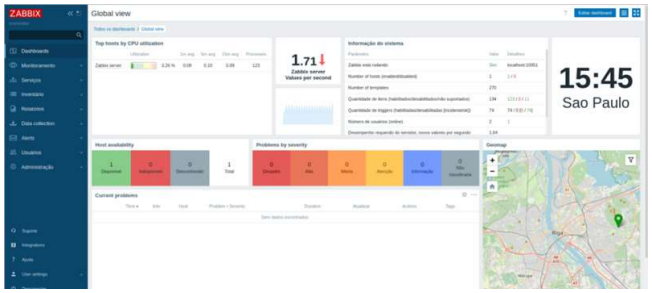
As configurações SNMP específicas do rádio Harris RF-7800V-HH incluem a escolha da versão do protocolo, a sequência de caracteres da comunidade SNMP, protocolos de autenticação e criptografia, senhas de autenticação e privacidade, permissão para enviar interceptações SNMP e o endereço IP de destino das interceptações. Essas configurações permitem ajustar a funcionalidade SNMP do rádio de acordo com as necessidades de gerenciamento e segurança, com ênfase na recomendação do uso da versão 3 do SNMP devido às suas medidas avançadas de segurança.

2.7 O SOFTWARE ZABBIX: CONCEITOS E FUNCIONAMENTO

O Zabbix (figura 01) representa uma solução de monitoramento para redes, servidores e serviços, desenvolvida com o propósito de supervisionar a disponibilidade, a experiência do usuário e a qualidade dos serviços.

A arquitetura do Zabbix e a versatilidade de seus módulos possibilitam a sua utilização em diversas áreas, incluindo o monitoramento convencional (verificação se está ativo ou inativo), o acompanhamento do desempenho de aplicações, a análise da experiência do usuário e a investigação das causas raiz em ambientes complexos, tudo isso por meio do servidor Zabbix e das regras de correlação.

Figura 01- Dashboard Zabbix



Fonte: Autor

Esta ferramenta de monitoramento de redes disponibiliza uma interface totalmente baseada na web para a administração e visualização de dados. Os alertas gerados pelo sistema de monitoramento Zabbix podem ser configurados para utilizar uma variedade de métodos de comunicação, como SMS, e-mail e até mesmo a criação de chamados em sistemas de suporte técnico. Além disso, o sistema permite a execução de ações automáticas, como o reinício de serviços, quando eventos específicos ocorrem.

O Zabbix oferece a opção de monitoramento sem a necessidade de instalar agentes em hosts, suportando vários protocolos, e possui funcionalidades de descoberta automática de itens (auto-discovery) e de descoberta de métricas em itens monitorados em níveis mais detalhados (low level discovery). Os principais componentes do sistema de monitoramento Zabbix incluem:

Zabbix Server: O servidor Zabbix coleta dados tanto de hosts com agentes instalados quanto de hosts sem agentes. Quando são identificadas irregularidades, alertas são acionados visualmente e por meio de diferentes canais de comunicação, como e-mail e SMS. No entanto, apenas o servidor Zabbix é necessário para sistemas Unix ou Linux.

Zabbix Proxy: O Zabbix Proxy coleta informações de uma parte do ambiente monitorado e repassa esses dados para o servidor Zabbix. Esse componente é essencial em arquiteturas de monitoramento distribuído e é especialmente útil em cenários com coleta assíncrona em redes distintas, onde não é viável manter regras de roteamento e firewall para cada host monitorado.

Zabbix Agent: O agente Zabbix é instalado nos hosts que se deseja monitorar e permite a coleta de métricas comuns específicas de um sistema operacional, como informações sobre CPU e memória. Além disso, o agente Zabbix permite a coleta de métricas personalizadas através do uso de scripts ou programas externos, possibilitando a captura de métricas mais complexas e até a execução de ações diretamente no agente Zabbix.

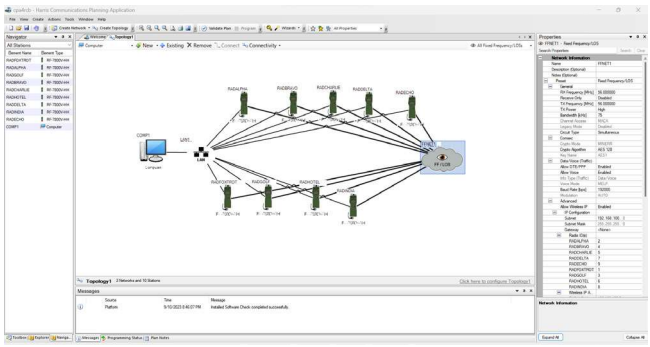
2.8 MONITORANDO O RÁDIO L3 HARRIS 7800V-HH COM O ZABBIX

Juntamente com uma variedade de opções adicionais, o dispositivo de comunicação de rádio L3 Harris 7800V-HH inclui a funcionalidade de supervisão através do protocolo SNMP (Protocolo de Gerenciamento de Rede Simples), nas versões 1, 2 ou 3. No seu Navegador de Arquivos, ele armazena os arquivos relacionados aos recursos disponíveis para acesso via SNMP (MIB - Management Information Base), permitindo a monitorização de recursos como potência, frequência, transmissão e recepção, bem como endereços de rede e uma ampla gama de informações relacionadas às configurações e ao desempenho do dispositivo em tempo real. É igualmente possível tomar ações sobre algumas dessas informações, tais como ajustar o volume, alterar o canal, modificar a potência e ativar o PTT do dispositivo, através do protocolo SNMP. No Zabbix, é viável criar itens e gatilhos que emitem alertas em tempo real acerca de quaisquer recursos disponíveis nas MIBs do dispositivo de rádio, incluindo a exibição de notificações sobre transmissões ou recepções de rádio, o monitoramento de endereços IP, bem como potência ou frequência de utilização.

O rádio é configurado através do software CPA (Communication Planning Application) (figura 02), o qual permite definir, com suporte gráfico e intuitivo, as topologias de redes e os hosts (rádios) ou outros dispositivos que estarão conectados a elas, bem como seus respectivos endereços IP. É criada uma topologia com frequência fixa, a qual possibilita comunicação de dados IP e voz, e dentre os parâmetros estabelecidos, é possível definir a versão do protocolo SNMP que será utilizada, bem como a comunidade SNMP que terá acesso aos recursos que o protocolo dispõe. Após

definir as configurações, gerar o arquivo de configuração e programar o equipamento rádio, este está em condições de ser um ativo participante da rede, bem como ser monitorado.

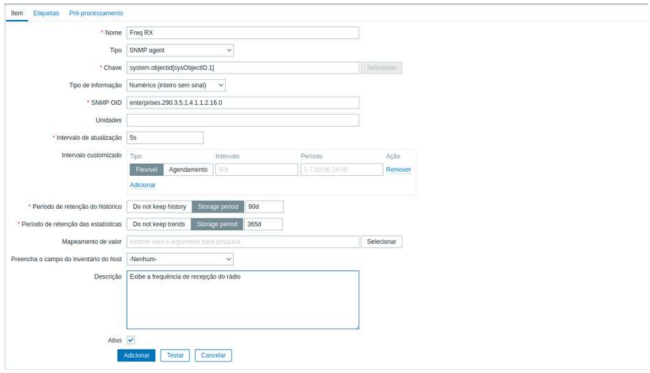
Figura 02 - Tela de configuração CPA



Fonte: Autor

No Zabbix são criados os itens (figura 02), nos quais são cadastrados os parâmetros referentes ao recurso que será monitorado, e posteriormente as respectivas triggers, as quais serão disparadas de acordo com o comportamento do equipamento rádio, gerando alertas na dashboard do zabbix, podendo ou não receber um tratamento via o recurso "action", e gerando um banco de dados de comportamento host monitorado.

Figura 03 - Criação de item para monitoramento de RX, via Zabbix.



Fonte: Autor.

Após realizadas as configurações, host adicionado e item e trigger criados, o rádio pode ser adicionado aos mapas de monitoramento, e a visualização dos eventos é possível também através da dashboard do Zabbix (figura 01).

Por ser considerado um ativo, ao estar conectado a uma rede, o dispositivo de rádio RF 7800V-HH se transforma em um elemento que requer o monitoramento dos seus recursos, assim como a avaliação das suas métricas, tanto para garantir a segurança e a estabilidade das conexões de dados, como para preservar a integridade da rede à qual está conectado.

3. CONCLUSÃO

Este artigo destacou a importância crítica do monitoramento do equipamento rádio L3 Harris 7800V-HH em infraestruturas de comunicação, especialmente em contextos militares e estratégicos. Este equipamento desempenha um papel fundamental na manutenção da conectividade e na garantia da eficiência das operações, tornando o monitoramento contínuo uma tarefa imperativa.

Além disso, exploramos o uso do software Zabbix como uma solução eficaz para monitorar o equipamento L3 Harris 7800V-HH. O Zabbix é uma ferramenta poderosa e versátil que permite às organizações monitorar de forma eficaz seus recursos de rede, garantindo um desempenho otimizado e a detecção precoce de problemas.

A relação entre o monitoramento de redes e a defesa cibernética também foi discutida, destacando como ambas as áreas desempenham papéis complementares na proteção contra ameaças cibernéticas. O monitoramento de redes, incluindo o uso do SNMP, desempenha um papel crucial na detecção de anomalias e no fornecimento de informações para a defesa cibernética agir proativamente.

Em resumo, o monitoramento constante do equipamento rádio L3 Harris 7800V-HH, combinado com o uso eficaz do software Zabbix e protocolo SNMP, é essencial para garantir a disponibilidade, desempenho e segurança das infraestruturas de comunicação em cenários críticos. Isso não apenas ajuda a manter operações fluidas e eficientes, mas também contribui para a segurança e o sucesso das missões e operações estratégicas.

Abstract

This work presents a suggestion for using the Zabbix software, an open source web application for monitoring network assets, with a specific focus on monitoring L3 Harris 7800V-HH radio equipment. Zabbix is a powerful and versatile tool that allows organizations to effectively monitor their network resources, ensuring optimized performance and early detection of problems. In this article, we will explore the essential functionalities of Zabbix, discuss its advantages and provide practical examples of its application in monitoring L3 Harris 7800V-HH equipment which is a critical asset in communications infrastructures.

Keywords: *Monitoring, Zabbix, L3 Harris 7800V-HH.*

4. REFERÊNCIAS

4-LINUX, **Software para monitoramento TI**. Disponível em: <https://4linux.com.br/software-free-open-source-para-monitoramento-ti/>. Acesso em 17 mai 23

4-LINUX, **O que é Monitoramento de TI**. Disponível em: <https://4linux.com.br/o-que-e-monitoramento-ti/>. Acesso em 10 jun 2023.

4-LINUX, **O que é SNMP**. Disponível em: <https://4linux.com.br/o-que-e-snmp/>. Acesso em: 20 jul. 2023.

DELFINO, Pedro. Snort: **A Solução Completa Para Monitorar Tráfego Em Redes**. Disponível em: <https://e-tinet.com/snort-monitor-redes/#:~:text=O%20Snort%20%C3%A9%20um%20sistema,TCP%20(Transmission%20Control%20Protocol).>. Acesso em 15 jul 23

DINIZ, Lucas Pimentel, e TAMIOSSO, Juliano Silva. **RÁDIO VHF RF-7800V-HH (FALCON III): INTEGRAÇÃO RÁDIO TELEFÔNICA - TRI**. 2020.

HARRIS CORPORATION RF COMMUNICATIONS DIVISION. **RF-7800V-HH: Rádio VHF portátil – manual de operações**. NY USA, 2012. Rev. E. Número da Publicação: 10515-0363-4204.

PINHEIRO, J. M. S. **Gerenciamento de Redes de Computadores: Uma Breve Introdução.** Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php>. Acesso em: 10 jun. 2023.

O 2º Sgt Lucas Pimentel **Diniz** é formado no Curso de Comunicações da Escola de Sargentos das Armas. Concluiu com aproveitamento o curso de Operador de Tecnologia da Informação e Comunicação e o curso de Proteção Cibernética. Atualmente, exerce a função de monitor de estabelecimento de ensino na Escola de Comunicações e pode ser contactado pelo email diniz.lucas@eb.mil.br.

O 2º Sgt Anderson **Lucio** Gomes é Técnologo em Jogos Digitais Pelo Instituto Federal do Mato Grosso do Sul. É formado no Curso de Comunicações da Escola de Sargentos das Armas. Atualmente, exerce a função de monitor de estabelecimento de ensino na Escola de Comunicações e pode ser contactado pelo email lucio.gomes@eb.mil.br.