ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

Cap QCO Infor DENIS LUCIO DE LIMA

IMPLANTAÇÃO DA FERRAMENTA ZABBIX NO CENTRO DE AVALIAÇÕES DO EXÉRCITO – CAEx, COMO PLATAFORMA DE GESTÃO E MONITORAMENTO DO AMBIENTE COMPUTACIONAL, NA PREVENÇÃO A SINISTROS NA REDE

Rio de Janeiro
2020

Cap QCO Infor DENIS LUCIO DE LIMA

IMPLANTAÇÃO DA FERRAMENTA ZABBIX NO CENTRO DE AVALIAÇÕES DO EXÉRCITO – CAEx, COMO PLATAFORMA DE GESTÃO E MONITORAMENTO DO AMBIENTE COMPUTACIONAL, NA PREVENÇÃO A SINISTROS NA REDE

Trabalho de Conclusão de Curso apresentado à Comissão de Avaliação de Trabalhos Científicos da Divisão de Ensino da Escola de Formação Complementar do Exército, como exigência parcial para a aprovação no Curso de Aperfeiçoamento Militar.

Aprovado em: 16 / Outubro /2020

CARLOS EDUARDO ARRUDA DE SOUZA – Maj – 1º Membro
Escola de Formação Complementar do Exército

ANDERSON BARROS TORRES – Maj – 2º Membro
Escola de Formação Complementar do Exército

PABLO EUGENIO COUTO SOUZA – Cap – 3º Membro
Escola de Formação Complementar do Exército

IMPLANTAÇÃO DA FERRAMENTA ZABBIX NO CENTRO DE AVALIAÇÕES DO EXÉRCITO – CAEx, COMO PLATAFORMA DE GESTÃO E MONITORAMENTO DO AMBIENTE COMPUTACIONAL, NA PREVENÇÃO A SINISTROS NA REDE

Denis Lucio de Lima[1]

RESUMO

O presente artigo tem como objetivo apresentar um estudo de caso da implantação da ferramenta Zabbix, como artifício para monitoramento e gestão do ambiente computacional do Centro de Avaliações do Exército – CAEx. Para essa finalidade, utilizou-se a observação de dados de saída coletados de um servidor, que abriga o sistema de protocolo eletrônico de documentos (SPED) e que opera nas dependências da Divisão de Tecnologia da Informação da Instituição, sendo gerenciado pela ferramenta Zabbix. Os resultados demonstraram que logo após a instalação da ferramenta e monitoramento do servidor SPED, foram emitidos alertas no painel de controle, informando que a capacidade de armazenamento do servidor estava comprometida. Alertas como esse, permitem ao administrador de redes tomar medidas proativas para sanar possíveis sinistros no ambiente de rede monitorado.

Palavras-chave: gestão, monitoramento, SPED, Zabbix.

ABSTRACT

This article aims to present a case study of the implementation of the Zabbix tool, as a device for monitoring and managing the computational environment of the Army Assessment Center - CAEx. For this purpose, we used the observation of output data collected from a server, which houses the electronic document protocol system (SPED) and which operates on the premises of the Institution's Information Technology Division, being managed by the Zabbix tool. The results showed that after the installation of the tool and monitoring of the SPED server, alerts were issued on the control panel, informing that the server's storage capacity was compromised. Alerts like this, allow the network administrator to take proactive measures to remedy possible claims in the monitored network environment.

Keywords: management, monitoring, SPED, Zabbix.

[1] Capitão QCO de Informática da turma de 2012. Especialista em Aplicações Complementares às Ciências Militares pela EsFCEx em 2012.

SUMÁRIO

1. INTRODUÇÃO

O presente artigo teve como objetivo apresentar um estudo de caso de implantação da ferramenta Zabbix, como artifício para monitoramento e gestão do ambiente computacional do Centro de Avaliações do Exército – CAEx. Essa OM tem como missão planejar, coordenar, controlar e executar avaliação e apreciação de Material de Emprego Militar, avaliação técnica de Produto Controlado pelo Exército, exame de valor balístico de munição e colaboração técnica envolvendo material de interesse do Exército.

O Exército Brasileiro, continuamente passa por uma transformação para se adaptar aos avanços tecnológicos e, várias medidas foram adotadas para fazer frente aos novos desafios impostos pela globalização e a revolução tecnológica. Diante disso, manter as infraestruturas de Tecnologia da Informação (TI) operacionais e com o menor tempo de indisponibilidade ganhou uma importância substancial, garantindo que os servidores e serviços presentes neste ambiente sejam minimamente afetados.

As Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro - IRESER (IR 13-15), de 31 de janeiro de 2007, têm como um de seus objetivos a “monitoração e registro de eventos referentes aos serviços corporativos de rede”. Nesse sentido a equipe de TI do CAEx promoveu uma pesquisa para verificar a viabilidade de uma ferramenta capaz de identificar de forma proativa os problemas e situações adversas do cotidiano, vividos pelos profissionais inseridos neste ambiente.

Diante disso, algumas indagações surgiram quanto à previsibilidade e ao tempo de reação aos sinistros ocorridos no ambiente de rede do CAEx. Seria possível monitorar e dar respostas mais rápidas a esses eventos? Como manter a disponibilidade e a confiabilidade dos serviços ofertados neste ambiente?

Com o propósito de responder a esses questionamentos, o presente trabalho visa a abordar a implantação e configuração da ferramenta Zabbix no CAEx, já que não há uma solução dedicada para este serviço em utilização na OM atualmente. Esta é uma ferramenta de código aberto e livre de qualquer custo envolvido. Ela é distribuída pela GNU (*General Public License*). É também um *software* que verifica vários parâmetros da rede, dos servidores e da saúde dos serviços.

O Zabbix é um *software* estável e apresenta relatórios muito bons. A ferramenta permite ainda o monitoramento a dispositivos remotos com ou sem o uso de agentes instalados, monitoramento de máquinas virtuais e de aplicações *web* (SOUZA, 2017).

Buscou-se, nesse trabalho, implantar e configurar no ambiente de rede do CAEx, um servidor com *Zabbix Server*. Componente esse que permite verificar serviços remotos como servidores *web*, dentre outros. Além disso, o *Zabbix Agent* fora instalado nos servidores monitorados. Para atingir esses objetivos, alguns conceitos importantes necessitam de uma compreensão maior para servir de arcabouço ao presente estudo. Dentre esses conceitos, cabe destacar o gerenciamento de redes, o protocolo TCP/IP, as *Management Information Base* – MIB, o protocolo *Simple Network Management Protocol* – SNMP, a diferença de gerente e agente no ambiente de monitoramento, as principais ferramentas de gerenciamento de redes do mercado, a ferramenta Zabbix propriamente dita e por fim, aspectos da instalação e configuração do Zabbix.

2. METODOLOGIA

O referencial teórico foi elaborado com o conteúdo obtido por meio de pesquisas a artigos, livros e documentos de referência relacionados ao tema do presente trabalho. A maior parte das buscas foram realizadas na plataforma Google Acadêmico, que proporciona uma pesquisa satisfatória para o referencial teórico do trabalho. Portarias normativas no âmbito do Exército Brasileiro também foram essenciais para nortear as pesquisas relacionadas a monitoramento de redes. Além disso, as documentações de referência disponíveis no *site* da ferramenta Zabbix contribuíram para o entendimento mais aprofundado da instalação e utilização do Zabbix. Em relação à estratégia para busca nessas bases, foram utilizados os seguintes termos descritores: “gerenciamento de redes”, "monitoramento de redes”, “soluções de monitoramento", “protocolos de rede”, “Zabbix” e “Nagios”. Como critérios de inclusão foram considerados estudos publicados em português e inglês que tratam da temática, além das orientações e publicações nos sítios de algumas das principais ferramentas de monitoramento do mercado (Zabbix, Nagios).

Com a finalidade de medir a eficiência, foi projetado um estudo de caso, onde observou-se o comportamento da solução proposta neste trabalho por um período de um mês. Esses dados de saída foram coletados de um servidor que abriga o sistema de protocolo eletrônico de documentos (SPED), que opera nas dependências da Divisão de Tecnologia da Informação do CAEx, sendo gerenciado pela ferramenta Zabbix.

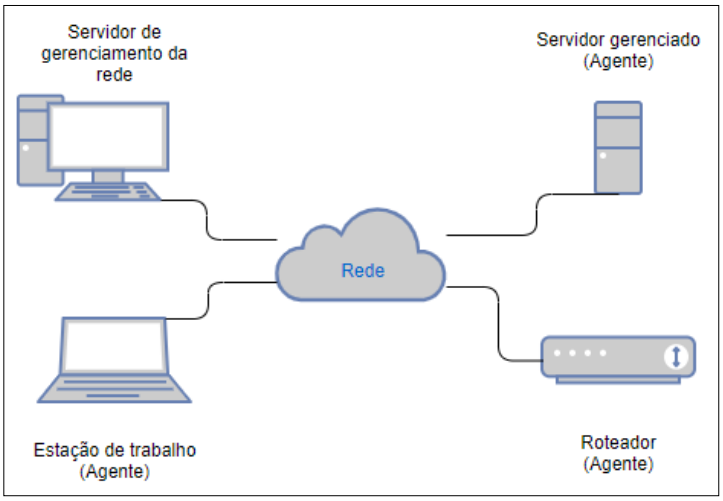
O restante do trabalho está organizado da seguinte maneira. No Capítulo 3, são apresentados conceitos de Gerenciamento de Redes e a ferramenta Zabbix propriamente dita. No Capítulo 4 observa-se os resultados alcançados com a implantação do Zabbix como ferramenta de monitoramento no CAEx. No Capítulo 5 é apresentada uma discussão sobre o emprego da ferramenta Zabbix no CAEx traçando um paralelo sobre como era realizado o monitoramento anteriormente à utilização desta ferramenta. Por fim no Capítulo 6 é apresentada a conclusão.

3. GERENCIAMENTO DE REDES

Não é de hoje que as redes de computadores estão ficando cada vez mais importantes para as organizações. Atualmente, é uma infraestrutura indispensável e de missão crítica, ou seja, não pode haver paralisação das atividades (LIMA, 2014).

A função do gerenciamento de redes é monitorar os equipamentos e meios de comunicação das redes, para detectar e corrigir problemas (Figura 1). Essa estratégia baseia-se na obtenção de informações dos dispositivos pertencentes às redes. Eles são analisados e os problemas que ocorrem são exibidos, além disso o volume de tráfego de dados pode ser monitorado, bem como é possível receber alertas de diferentes dispositivos, que possibilitam um diagnóstico e capacidade de solução na administração do ambiente monitorado (SOUZA, 2017).

Figura 1 – Gerenciamento de redes



Fonte: Elaborado pelo autor

3.1 PROTOCOLOS E ELEMENTOS DE UM SISTEMA DE GERENCIAMENTO DE REDES

3.1.1 TCP/IP

Nos primórdios da criação da internet, diversas universidades e repartições públicas foram conectadas, mas problemas de comunicação surgiram, pois não havia uma padronização de protocolos. Com esse impasse, um modelo de referência passou a ser adotado, o chamado Modelo de Referência TCP/IP, utilizando uma pilha de protocolos TCP/IP, que permitiu que os computadores de uma rede pudessem se comunicar. A composição desse modelo apresenta as seguintes camadas: aplicação, transporte, rede e acesso à rede. Em cada camada atuam determinados protocolos que interagem com os protocolos das outras camadas desta arquitetura, permitindo que os dados trafeguem por todo o ambiente de rede (TANENBAUM, 2003).

3.1.2 SNMP

O Agente SNMP "*Simple Network Management Protocol"* é um programa ou aplicação executado nos dispositivos de rede e que envia informações ao gerenciador central.

Os dispositivos gerenciados possuem um agente SNMP e uma base de dados chamada de MIB (*Management Information Base*), que contém informações de gerenciamento que refletem sua configuração e o seu comportamento, além de parâmetros que podem ser usados para gerir suas operações. Portanto, um agente SNMP pode receber solicitações de leitura e gravação de dados na mib, e gerar um alerta para o gerente SNMP no caso de algum parâmetro alcançar algum limite preestabelecido (ZELTSERMAN,1999).

Chama-se a operação de *trap,* quando o agente envia as informações para o servidor central sem a necessidade de uma solicitação. Já o *polling*, é quando o servidor central faz as solicitações periodicamente ao agente ou agentes. Todo esse controle e transporte é realizado pelo protocolo SNMP.

Quando o equipamento que se deseja monitorar não possui o agente SNMP, a solução encontrada é verificar se eles estão ativos ou não, utilizando o protocolo ICMP "*Internet Control Message Protocol*"(*ping*). Nessa estratégia, o servidor central envia o comando *ping* para o IP do dispositivo remoto e aguarda a resposta a esse comando. Esse teste indicará se o dispositivo está ativo ou não.

3.1.3 MIB

As MIB são um conjunto de objetos gerenciados, que englobam todas as informações necessárias para a gerência da rede. Esses objetos gerenciados podem ter permissões para serem lidos ou alterados (DIAS; ALVES JÚNIOR, 2001).

As normas e os padrões utilizados na criação de uma MIB foram descritos nas publicações RFC1066 e RFC1156 para a MIB-I e posteriormente as RFC1158 e RFC1213 para a MIB-II, que foi expandida e melhorada. A MIB-II, que é o padrão atual, contém informações como: nome, endereço, número de portas, entre outros dados sobre os objetos gerenciados.

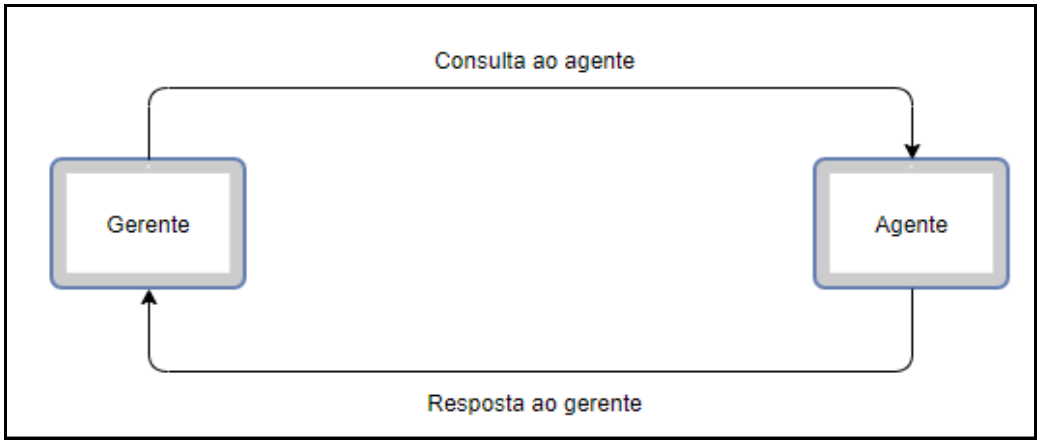
Uma MIB é estruturada em forma de árvore de dados, chamada de Árvore de Nomeação Global. Cada nó possui um identificador chamado de OID. Para cada OID numérico vindo dos dispositivos monitorados, a MIB traduz para uma mensagem de texto correspondente, especificando o que significa cada alerta.

3.1.4 GERENTE E AGENTE

Em um sistema de gerenciamento de redes, o gerente é o dispositivo central, que recebe todas as informações de gerenciamento provenientes dos agentes e apresentadas amigavelmente por meio de gráficos e relatórios (SOUZA, 2017).

De acordo com DIAS e ALVES JÚNIOR (2001), o agente é um processo executado no dispositivo gerenciado e que possui algumas tarefas importantes como: atender as requisições enviadas pelo gerente (*polling*) e enviar automaticamente informações de gerenciamento para o gerente (*trap*).

Figura 2 – Gerente e agente



Fonte: Elaborado pelo autor

3.2 PRINCIPAIS FERRAMENTAS NO MERCADO

Atualmente existem inúmeras ferramentas de gerenciamento de redes no mercado, cada uma delas com suas peculiaridades. Será apresentado a seguir as principais ferramentas de gerenciamento bem como seus pontos fortes.

Na presente pesquisa abordaremos as seguintes ferramentas no mercado: Cacti, Nagios e Zabbix. Todas essas soluções são gratuitas, sendo distribuídas sob a licença GNU GPL.

O Cacti é uma ferramenta que exibe informações sobre o estado da rede de computadores por meio de gráficos. Monitora o estado dos elementos da rede e programas, bem como a largura de banda utilizada e uso de CPU.

Como desvantagem, o produto não possui um agente de descoberta automático, fazendo com que o administrador da rede tenha que adicionar manualmente os elementos que se deseja monitorar e caso a rede seja muito grande esse trabalho será bastante penoso (BLACK, 2008).

O Nagios é um aplicativo de monitoramento de sistemas e de redes. Ele verifica clientes e serviços especificados, emitindo alertas quando alguma situação fora dos padrões pré-definidos ocorre. Originalmente foi desenvolvido para operar em sistemas Linux. (BLACK, 2008).

O Zabbix é uma ferramenta de gerenciamento de redes para todos os portes, seja uma rede simples ou uma grande rede complexa. Possui uma variedade de opções e é responsável por cobrir lacunas deixadas por seus concorrentes, fazendo com que os administradores de rede tivessem que utilizar duas ou mais ferramentas para atingir os mesmos objetivos.

O Zabbix é um *software* que pode funcionar de maneira redundante, em mais de um servidor, recolhendo os dados gerados pelos agentes que operam nos diversos clientes. Seus dados podem ser armazenados em diversos bancos de dados relacionais. Seus agentes estão disponíveis para sistemas operacionais Linux, Unix, MacOS X, Solaris, FreeBSD, Netware, Windows e dispositivos rodando SNMP v1, v2 e v3. (BLACK, 2008).

3.3 A FERRAMENTA ZABBIX

A ferramenta Zabbix auxilia no monitoramento de rede, além de afiançar melhor performance e disponibilidade para os todos serviços e ativos inerentes ao ambiente computacional. Nesta análise são envolvidas todas aplicações e integração dos equipamentos interligados a ela, dentre eles, *hosts*, servidores, roteadores, *switches* e outros (GALIANO FILHO, 2010).

O Zabbix é um sistema que coleta informações dos dispositivos que encontram-se interligados na rede e essas informações são absorvidas através de *scripts*, via agente pelo *Simple Network Management Protocol* (SNMP) (GALIANO FILHO, 2010).

Esse sistema de gerência e monitoramento tem a capacidade para inspecionar praticamente qualquer evento na rede, desde o tráfego da rede, até quantos papéis restam na impressora. É o *software* de nível corporativo ideal para o acompanhamento, em tempo real, de milhões de métricas coletadas de dezenas de milhares de servidores, máquinas virtuais e dispositivos de rede (ZABBIX, 2020).

A aplicação Zabbix é difundida com a administração centrada via navegador web e o armazenamento dos dados são reunidos em um banco de dados relacional, com suporte às três versões do protocolo SNMP. A ferramenta tem um agente compatível com diferentes sistemas operacionais como: Solaris, Linux, HP-UX, OS X, Open BSD, NT4.0, Windows 7, Windows XP (SILVA; MEDEIROS; MARTINS, 2015).

Observa-se que o Zabbix aprovisiona diferentes meios de realizar o monitoramento dos aspectos da infraestrutura de TI e, de fato, quase tudo o que pode se conectar a ela. Pode ser assinalado como um sistema de monitoramento semi-distribuído com gerenciamento centralizado.

Cabe salientar que há uma dependência em detrimento da estrutura do Zabbix, já que esta ferramenta foi projetada com objetivo de ser uma ferramenta *Open Source*, com isso, o servidor essencialmente deve ser hospedado em uma máquina baseada em Linux ou Mac OS, já que não há um pacote do servidor disponível para as versões do Windows. Apesar disso, essa dependência não tende afetar a realização do monitoramento da rede, pois o sistema encontra-se divido em três partes distintas: Servidor Zabbix; Agente Zabbix e Interface do Zabbix (GALIANO FILHO, 2010).

a) Servidor Zabbix: tem a função de coletar e armazenar dados monitorados. Por isso, o servidor deve ser essencialmente hospedado em uma máquina com o sistema operacional fundamentado na família do Unix (Linux ou Mac OS) (GALIANO FILHO, 2010).

b) Agente Zabbix: tem a função de repassar todas as informações que foram coletadas pelo sistema operacional, no qual está em operação e as envia para o

servidor central. Ele continua instalado na máquina a fim de ser executado como *daemon* ou serviço, e tão logo, o servidor solicite alguma requisição, o agente incumbe-se do processamento, requisição e retorno dos dados solicitados, como: memória, consumo dos recursos de HD, estatística de processador, dentre outros (GALIANO FILHO, 2010).

c) Interface do Zabbix: configura-se como uma estrutura que consente que o administrador possa acessar, interagir e administrar o sistema. Ela permite um fácil acesso ao monitoramento dos dados e configurações por meio do Zabbix, foi projetada para acesso via *web* (GALIANO FILHO, 2010).

3.4 CONSIDERAÇÕES FINAIS

O emprego do *software* de gerenciamento de redes é um meio que permite ao administrador de redes identificar problemas em tempo hábil para saná-los e minimizar o tempo de indisponibilidade dos serviços na rede. As principais ferramentas de monitoramento baseiam-se particularmente no protocolo SNMP.

À medida que os ambientes de TI se tornam maiores e mais complexos, o monitoramento e os alertas se tornam um componente essencial para garantir que os sistemas permaneçam *online* e saudáveis. Ao coletar dados sobre o estado do sistema, o administrador de rede pode ser notificado se um *host* ficar inoperante ou receber um aviso prévio de um problema iminente, como um disco ficando sem espaço. O armazenamento desses dados permite que o administrador de rede os analise posteriormente para solucionar problemas mais complexos ou transitórios, correlacionando dados de várias fontes para obter uma imagem mais clara de como os componentes do ambiente estão interagindo.

Dentre as várias ferramentas de gerenciamento de redes, suas possibilidades e fraquezas, quando comparadas, optou-se por utilizar a ferramenta Zabbix, como estudo de caso no CAEx.

No próximo capítulo serão apresentados os resultados alcançados com a implantação do Zabbix.

4. RESULTADOS

Como já citado anteriormente, o ambiente monitorado foi a rede de dados do Centro de Avaliações do Exército – CAEx, Barra de Guaratiba – RJ. Este ambiente é composto por computadores, servidores e *switchs* interligados fisicamente baseado no modelo Ethernet. A ligação entre o *switch* core e os *switchs* de distribuição se dá por meio de fibra ótica.

O servidor onde foi instalado o Zabbix (gerente) está situado na Divisão de Tecnologia da Informação do CAEx, por meio do qual os dados dos dispositivos da rede monitorada são coletados através do protocolo SNMP. Desta maneira foi necessário realizar a instalação do agente SNMP nos computadores monitorados.

Para se fazer a implantação e configuração no ambiente de rede do CAEx, com *Zabbix Server*, foi realizada a instalação do mesmo, como uma solução proativa, traçando um paralelo sobre como era realizado o monitoramento anteriormente à utilização desta ferramenta.

4.1 DETALHAMENTO DO ESTUDO DE CASO

O estudo de caso iniciou-se com a instalação do Zabbix *Server.* Conforme o *site* oficial do Zabbix, os recursos necessários variam de acordo com o número de *hosts* monitorados e para o cenário do CAEx os recursos exigidos são mínimos. Entretanto, o servidor utilizado possui boas configurações e já abriga outros serviços da rede e seus recursos computacionais ainda poderiam ser melhores utilizados.

Complementando o estudo de caso, foi necessário realizar a instalação do Zabbix *Agent* no servidor SPED, equipamento este que passaria a enviar os dados de interesse para o monitoramento.

O SPED é um dos módulos componentes do Projeto do Sistema Informatizado de Gestão Arquivística e Documental do Exército (SIGADEx). Além

deste componente, existem ainda o Módulo Integrador, *Workflow* (fluxo de trabalho), Formato Eletrônico e Certificação Digital.

São objetivos do SPED, a adoção de um sistema único de gerenciamento eletrônico de documentos utilizado por toda a Força Terrestre, a padronização do processo de gerenciamento eletrônico de documentos (confecção, protocolo e expedição) e a implantação do Número Único de Documentos (NUD).

Devido a importância do SPED, se faz necessário monitorar o servidor que o hospeda. Pois toda a documentação, com seus despachos e encaminhamentos, que circula no âmbito de uma OM, como o CAEx, obrigatoriamente utiliza-se desse sistema como fluxo documental.

Para o experimento foi necessário apenas instalar os pacotes do Zabbix *Server* via Terminal do Linux, com privilégios de administrador e também os pacotes de instalação do Zabbix *Agent* no servidor monitorado.

4.1.1 DADOS DO SERVIDOR

Abaixo, *script* das imagens do servidor.

Figura 3 – Processador

```
# cat /proc/cpuinfo
cpu cores: 10
vendor_id: GenuineIntel
cpu MHz: 1260.384
cache size: 25600 KB
model name: Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz
```

Fonte: Elaborado pelo autor

Figura 4 – Memória

```
# cat /proc/meminfo
MemTotal:     16328900 kB
MemFree: 234168 kB
MemAvailable: 14144616 kB
```

Fonte: Elaborado pelo autor

Figura 5 – Armazenamento

```
# df
Sist. Arq.                Tam.   Usado   Disp.   Uso%   Montado em
udev                      7,8G   0       7,8G    0%     /dev
tmpfs                     1,6G   166M    1,4G    11%    /run
/dev/sda6                 1,1T   482G    613G    45%    /
tmpfs                     7,8G   0       7,8G    0%     /dev/shm
tmpfs                     5,0M   0       5,0M    0%     /run/lock
tmpfs                     7,8G   0       7,8G    0%     /sys/fs/cgroup
/dev/mapper/mpathd-part1  2,7T   944G    1,8T    35%    /mnt/dg01_v0001
tmpfs                     1,6G   0       1,6G    0%     /run/user/0
```

Fonte: Elaborado pelo autor

Figura 6 – Kernel do Linux

```
# cat /proc/version
Linux version 4.19.0-10-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP Debian 4.19.132-1
```

Fonte: Elaborado pelo autor

Figura 7 – Versão do Sistema Operacional

```
# cat /etc/issue
Debian GNU/Linux 10 \n \l
```

Fonte: Elaborado pelo autor

4.1.2 INSTALAÇÃO DO SERVIDOR ZABBIX

Figura 8 – Instalação dos pacotes do *Zabbix Server*

```
#  apt update
#  apt install zabbix-server-mysql zabbix-frontend-php zabbix-cli python-socks python-ntlm snmptrapd snmp-mibs-downloader zabbix-agent
```

Fonte: Elaborado pelo autor

Não foi necessário instalar o Apache e PHP, pois estes pacotes já haviam sido instalados no servidor anteriormente para utilização de outros serviços.

O banco de dados utilizado foi o MariaDB, que também já estava instalado no servidor em questão, mas foi necessário criar a base de dados para o Zabbix, como veremos a seguir.

Figura 9 – Criação da base dados

```
#  mysql -u root -p
>  create database zabbix character set utf8 collate utf8_bin;
>  grant all privileges on zabbix.* to zabbix@localhost identified by <SENHA DO BD>;
>  quit;
#  zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -u zabbix -p
```

Fonte: Elaborado pelo autor

Em seguida, o *daemon* do servidor Zabbix para usar o banco de dados criado precisou ser editado.

Figura 10 – Parâmetro do *daemon* do servidor Zabbix

```
# vim /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbix
```

Fonte: Elaborado pelo autor

Iniciando o serviço no *Zabbix server*:

Figura 11 – Inicialização do serviço Zabbix

```
# service zabbix-server start
```

Fonte: Elaborado pelo autor

Reiniciando o serviço do servidor Apache:

Figura 12 – Inicialização do Apache *server*

```
# service apache2 restart
```

Fonte: Elaborado pelo autor

4.1.3 INSTALAÇÃO DO ZABBIX AGENTE NO SERVIDOR SPED

Figura 13 – Instalação dos pacotes Zabbix Agent

```
# apt-get install zabbix-agent
```

Fonte: Elaborado pelo autor

Figura 14 – Cópia do arquivo de configuração do Zabbix Agent:

```
# mv /etc/zabbix/zabbix_agentd.conf /etc/zabbix/zabbix_agentd.conf_original
```

Fonte: Elaborado pelo autor

Figura 15 – Criação do novo arquivo de configuração:

```
# touch /etc/zabbix/zabbix_agentd.conf
```

Fonte: Elaborado pelo autor

Figura 16 – Inserção dos parâmetros no novo arquivo:

```
Server=127.0.0.1, <Ip do Servidor Zabbix>
ServerActive=<Ip do Servidor Zabbix>
StartAgents=5
DebugLevel=3
LogFile=/var/log/zabbix-agent/zabbix_agentd.log
Timeout=3
```

Fonte: Elaborado pelo autor

Figura 17 – Reiniciando o serviço do Zabbix Agente:

```
# service zabbix-agent stop
# service zabbix-agent start
```

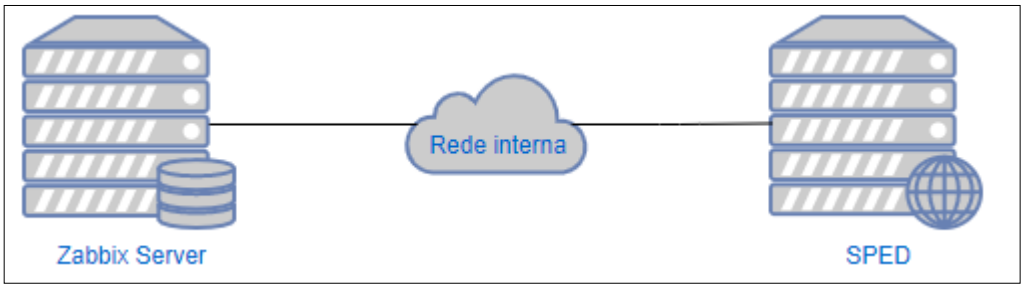
Fonte: Elaborado pelo autor

4.2 APLICAÇÃO DA METODOLOGIA

Como demonstrado acima, a instalação do Zabbix ocorreu em equipamentos distintos, um que assumiu o controle pelo monitoramento, o Servidor Zabbix e outro como equipamento monitorado, neste caso o servidor SPED.

A Figura 18 ilustra o monitoramento do Zabbix Server com o equipamento monitorado.

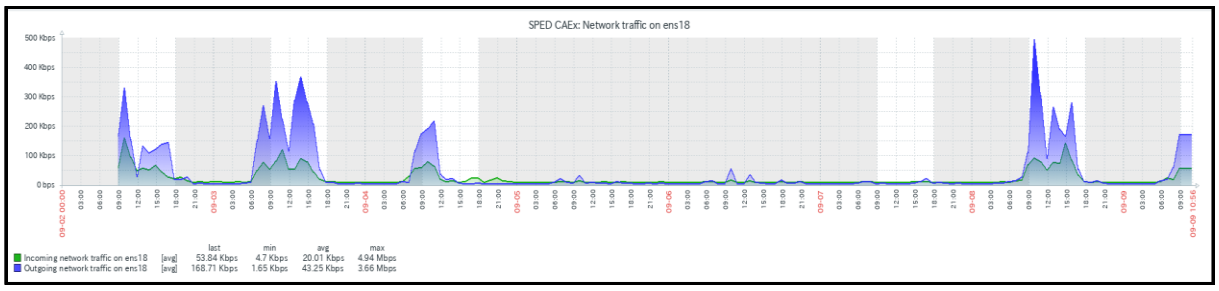
Figura 18 – Esquema de rede



Fonte: Elaborado pelo autor

O primeiro resultado pode ser verificado na Figura 19, que forneceu informação sobre o tráfego na interface de rede do servidor SPED. Não houve interrupção do serviço, apenas foi constatado uma diminuição no tráfego da rede durante o período do final de semana.

Figura 19 – SPED: Tráfego de Rede



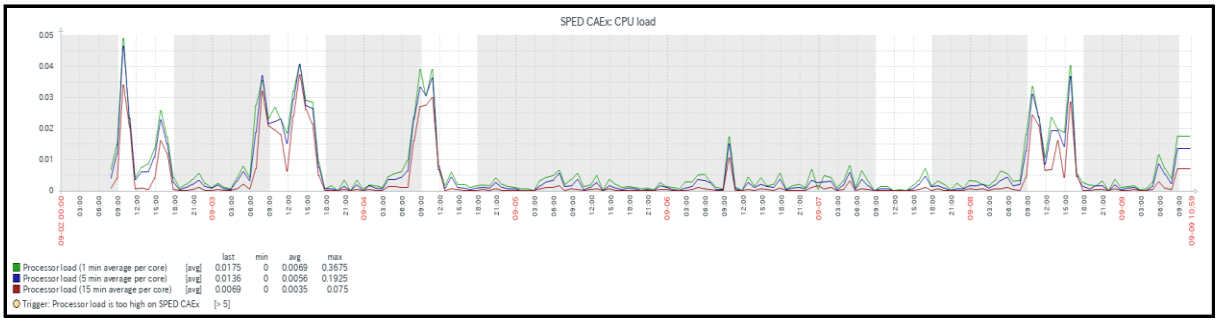
Fonte: Elaborado pelo autor

Por intermédio da Figura 19 também observa-se que houve um pico de 4.94Mbps, decorrente do grande acesso de usuários ao SPED.

Ao se comparar a Figura 19 com a Figura 20, pode ser observado que o uso de CPU do Servidor Zabbix e o tráfego da rede são bem parecidos, ou seja, há uma grande utilização desses recursos durante o dia, e há uma ligeira baixa dessa utilização durante o final do expediente, e nos finais de semana.

Cabe ressaltar que o livro de partes do Oficial-de-Dia é produzido eletronicamente no SPED, por isso, percebe-se um discreto aumento no uso de CPU e recursos de rede durante o final de semana.

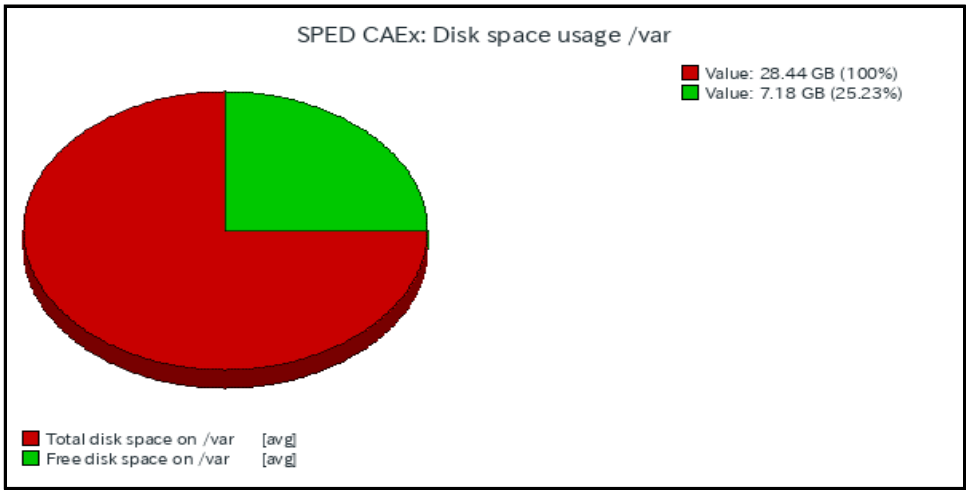
Figura 20 – SPED: Uso de CPU



Fonte: Elaborado pelo autor

A Figura 21 ilustra a capacidade de armazenamento do disco rígido na partição /var do servidor SPED, além de seus percentuais de utilização. A partição de tamanho de 28.44 Gb apresentou 7.18 Gb (25.23%) de espaço disponível, após intervenção do gerente de redes, que constatou alarme no início de seu monitoramento pela supracitada ferramenta.

Figura 21 – SPED: Espaço em Disco



Fonte: Elaborado pelo autor

A medição realizada pelo Servidor Zabbix permitiu configurar um gatilho (trigger), cujo parâmetro foi de 80% de utilização da partição. Os alarmes foram exibidos no painel de controle da ferramenta, permitindo que a equipe de gerência realizasse procedimentos preventivos, para mitigar uma possível extrapolação de espaço da partição citada. A Figura 22 ilustra o alerta, concomitantemente sanado pelos responsáveis pelo monitoramento.

Figura 22 – Alerta: Espaço em partição inferior a 20%

Fonte: Elaborado pelo autor

5. DISCUSSÃO

Com a implementação da ferramenta Zabbix, o estudo deixa explícito que as principais demandas levantadas, como gerenciamento e monitoramento de ativos de rede, foram alcançadas, fornecendo informações dos componentes da rede, auxiliando o gerente a tomar decisões mais assertivas.

No ambiente de estudo (CAEx), não havia ferramenta de monitoramento de redes. A atuação do gerente se dava na resolução de problemas já ocorridos. Essa forma reativa de trabalhar gerava um tempo de resposta maior do que o necessário para tratamento dos incidentes, pois não havia maneiras de se antecipar aos possíveis problemas que poderiam ser causados na rede.

Portanto, a aplicação do Zabbix permitiu uma ação mais rápida na identificação do problema, para posterior planejamento de ações, de curto e médio prazos. Essas informações reduzem os deslocamentos *in loco* para identificação das ocorrências, bem como ajustes na configuração dos ativos para adequação das futuras necessidades da OM.

Outro resultado de impacto foi que logo após a instalação da ferramenta e monitoramento do servidor SPED, foram emitidos alertas no painel de controle de que a partição /var se encontrava com sua capacidade de armazenamento comprometida. A medida para mitigar o problema identificado foi a transferência dos dados de *log* para outra partição com maior capacidade.

Para o atendimento das principais questões identificadas, a ferramenta Zabbix atuou diretamente na elucidação de problemas, o que a habilita como uma solução viável para o estudo de caso proposto.

6. CONCLUSÃO

O presente trabalho apresentou uma proposta de implantação da ferramenta Zabbix, como artifício para monitoramento e gestão do ambiente computacional do Centro de Avaliações do Exército – CAEx.

Foi comprovada a eficácia na utilização da ferramenta, como suporte para gestão e monitoramento, bem como na possibilidade do setor de TI vislumbrar uma diretriz e planejamento para eventuais intercorrências na rede, oferecendo estratégias de forma proativa.

Monitorar dados de armazenamento foi bastante oportuno, pois possibilitou a identificação de uma real falta dos recursos na partição /var, o que permitiu a atuação da equipe de TI.

Como caso concreto, monitorar o servidor SPED foi de grande valia, pois acrescentou conhecimento no gerenciamento de um serviço que é utilizado por todo o Exército Brasileiro. Fica claro que esta prática pode ser bastante relevante para outras OM que pretendem monitorar seus ativos, pois este estudo ajudará e minimizará o retrabalho para configurar e monitorar tal aplicação.

Ao implantar a ferramenta Zabbix e monitorar o servidor SPED, a equipe de TI pôde obter informações extremamente relevantes de utilização de consumo de CPU, medição do tráfego de rede e espaço em disco, como já ilustrado nos resultados do trabalho. Esta poderosa ferramenta também permite a inclusão de parâmetros, gatilhos (*triggers*), que alertam o gerente quando estas condições são atingidas.

Apesar desta declaração não ser nova, este estudo deixa ainda evidente a necessidade de toda OM ter uma ferramenta de gerenciamento e monitoramento de ativos de rede, para promover o auxílio necessário aos integrantes da equipe de TI, na tomada de decisão, não somente de forma corretiva, mas preventiva.

Diante do curto período implantação e monitoramento pela ferramenta Zabbix no CAEx, o presente estudo limitou-se a coleta de informações básicas do ambiente monitorado, mas as possibilidades são grandes, como por exemplo, o envio de alertas para o gerente de redes caso algum gatilho de monitoramento seja atingido, dentre outros.

Como perspectivas para trabalhos futuros, sugere-se que sejam realizados estudos quanto a criação de *templates* customizados, que viabilizem a captura eventos específicos no dispositivo monitorado, permitindo a realização de ações específicas para determinado tipo de situação.

REFERÊNCIAS

BLACK. T. L. **Comparação de Ferramentas de Gerenciamento de Redes**. Porto Alegre, dezembro de 2008. Disponível em: < https://www.lume.ufrgs.br /handle /10183 /15986 >. Acesso em: 25 de ago. 2020.

DIAS, B. Z.; ALVES JUNIOR, N. **Protocolo de gerenciamento SNMP.** 2001. Disponível em: <http://www.rederio.br/downloads/pdf/nt00601.pdf>. Acesso em: 4 jul. 2020.

GALIANO FILHO, A. **Zabbix**: Ferramenta de Monitoramento. Curso de Especialização em Redes e Segurança de Sistemas Pontifícia Universidade Católica do Paraná Curitiba, abril de 2010. Disponível em:< https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08B/Adilson%20Galiano%20-%20Artigo.pdf>. Acesso em: 11 de jul. 2020.

LIMA, J. R. **Monitoramento de Redes com Zabbix** – Monitore a saúde dos servidores e equipamentos de rede. Rio de Janeiro: Brasport, 2014.

BRASIL. Exército. Portaria nº 004-DCT, de 31 de janeiro de 2007. Aprova as Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro - **IRESER (IR 13-15)**. Boletim do Exército, Brasília, DF, n.10, p.16, 9 de mar. 2007.

MCCLOGHRIE, K., and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets", **RFC 1066**, TWG, August 1988. Disponível em: <https://tools.ietf.org/html/rfc1066>. Acesso em: 4 de jul. 2020.

MCCLOGHRIE, K., and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets", **RFC 1156**, Performance Systems International and Hughes LAN Systems, May 1990. Disponível em: <https://tools.ietf.org/html/rfc1156>. Acesso em: 4 de jul. 2020.

MCCLOGHRIE, K., and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", **RFC 1213**, Performance Systems International, March 1991. Disponível em: <https://tools.ietf.org/html/rfc1213>. Acesso em: 4 de jul. 2020.

ROSE, M. "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", **RFC 1158**, Performance Systems International, May 1990. Disponível em: <https://tools.ietf.org/html/rfc1158>. Acesso em: 4 de jul. 2020.

SILVA, W. M. C; MEDEIROS, R.M; MARTINS, R.S. **Análise e gerenciamento de redes usando uma metodologia proativa com Zabbix**. HOLOS, Ano 31, Vol. 8, dezembro, 2015. Disponível em:< http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/2441>. Acesso em: 4 de jul. 2020.

SOUZA, L. B. **Gerenciamento e segurança de redes:** Tecnologia da Informação. São Paulo: SENAI, 2017.

TANENBAUM, A. S. **Redes de Computadores.** 4.ed. ed. Rio de Janeiro: Campus, 2003.

YIN, R. **Estudo de caso: planejamento e métodos.** 5. ed. Porto Alegre: Bookman, 2015.

ZABBIX. **Manual do Zabbix**. Zabbix SIA. Last update: 2019/10/07. Disponível em: <https://www.zabbix.com/documentation/current/pt/manual>. Acesso em: 1 de jun. 2020.

ZELTSERMAN, D. **A Practical Guide to SNMPv3 and Network Management.** São Paulo: Prentice-Hall. 1999.