ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

ESCOLA DE FORMAÇÃO COMPLEMENTAR DO EXÉRCITO

Cap QCO Infor Carlos Felipe da Rosa

UTILIZAÇÃO DO ZABBIX PARA GESTÃO E MONITORAMENTO DE ATIVOS DE REDE

Rio de Janeiro
2018

Cap QCO Infor CARLOS FELIPE DA ROSA

UTILIZAÇÃO DO ZABBIX PARA GESTÃO E MONITORAMENTO DE ATIVOS DE REDE

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares

Orientador: Maj Luiz Fernando Sousa da Fonte

Rio de Janeiro
2018

Cap QCO Infor CARLOS FELIPE DA ROSA

UTILIZAÇÃO DO ZABBIX PARA GESTÃO E MONITORAMENTO DE ATIVOS DE REDE

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares

Aprovado em

COMISSÃO DE AVALIAÇÃO

_____

Luiz Fernando Sousa da Fonte – Maj QCO Infor – Presidente
Escola de Formação Complementar do Exército

_____

Marcelo Antonio do Nascimento – Maj QCO Infor – Membro
Escola de Formação Complementar do Exército

UTILIZAÇÃO DO ZABBIX PARA GESTÃO E MONITORAMENTO DE ATIVOS DE REDE

Carlos Felipe da Rosa[a]

RESUMO

Monitorar uma rede é verificar a eficácia do funcionamento de cada serviço, equipamento e processos existentes em uma mesma infraestrutura. O monitoramento de uma rede de computadores torna-se uma atividade essencial com a finalidade de garantir o seu funcionamento contínuo como também para assegurar um elevado grau de qualidade dos serviços oferecidos. Devido a constante expansão do uso das redes de computadores, aumentam também os problemas, tais como: indisponibilidade de aplicação e/ou serviço, servidor de rede com baixa capacidade de processamento, entre outros. Diante disso, o monitoramento em tempo real da infraestrutura de rede e seus ativos, vêm se tornando indispensável na gestão da tecnologia da informação. Esse monitoramento permite obter de modo rápido, preciso e confiável as informações necessárias sobre esses equipamentos, facilitando as tomadas de decisões no momento do planejamento, adequação e expansão do ambiente computacional. Com isso, propõe-se implementar uma arquitetura baseada em um modelo Gerente-Agente para permitir a automação da coleta dos dados de diversos componentes de uma rede de computadores, visando ampliar a aplicação das métricas e auxiliar no gerenciamento e monitoramento. Uma ferramenta que ofereça e efetue essa coleta automatizada dos dados será implantada na rede de computadores do Comando de Operações Terrestres - COTER. Dentre as ferramentas existentes com estas características, a escolhida para essa tarefa é o Zabbix devido o licenciamento GPLv2, a gama de sistemas operacionais que é possível implantar os agentes e as diversas formas de notificações de alertas escalonadas.

Palavras-chave: monitoramento, gerenciamento, rede de computadores, tempo real, ativos de rede, gerente-agente, métrica.

ABSTRACT

Monitor a network is to verify the effective operation of each service, equipment and existing processes in the same infrastructure. The monitoring of a computer network becomes an essential activity to thus ensure its continued operation as well as to ensure a high level of quality of services offered. Due to constant expansion of the use of computer networks, also increase the problems, such as unavailability of application and / or service network server with low processing power, among others. Thus, the real-time monitoring of network infrastructure and its assets have become indispensable in the management of information technology. This monitoring allows for fast, precise and reliable information needed on such equipment, facilitating decision-making at the planning, adaptation and expansion of the computational environment. With this, it is proposed to implement an architecture based on a Manager-agent model to allow the automation of data collection of various components of a computer network, aiming to expand the application of metrics and assist in management and monitoring. A tool that offers and make this automated data collection will be located in the Land Operations Command - COTER computer network. Among the existing tools with these features, chosen for this task is Zabbix because the GPLv2 license, the range of operating systems that you can deploy the agents and the various forms of staggered alert notifications.

Keywords: monitoring, management, computer network, real-time, network assets, managing agent, metric.

---

[a] Capitão QCO de Informática da turma de 2010. Especialista em Aplicações Complementares às Ciências Militares pela EsFCEx em 2010.

SUMÁRIO

UTILIZAÇÃO DO ZABBIX PARA GESTÃO E MONITORAMENTO DE ATIVOS DE REDE

1. INTRODUÇÃO

O presente trabalho teve como objetivo apresentar ao leitor um estudo de caso de implementação e configuração da ferramenta Zabbix como plataforma de gerenciamento e monitoramento de um ambiente computacional em uma Organização Militar – OM do Exército Brasileiro.

A evolução da computação determinou que as OM do Exército Brasileiro fossem dotadas de equipamentos de Tecnologia da Informação – TI. Esta imposição trouxe consigo a necessidade de manter uma infraestrutura de TI com alto índice de disponibilidade, em função dos serviços e sistemas debruçados naquele pilar.

O Comando de Operações Terrestres – COTER, Órgão de Direção Operacional – ODOp do Exército Brasileiro sentiu a necessidade de gerenciar e monitorar seus ativos de rede após um crescimento de suas demandas na área de tecnologia da informação, impostas pelo incremento de atividades designadas ao ODOp nos últimos anos por força da transformação da Força Terrestre.

Desta forma, a área responsável pela TI do COTER indagou-se sobre quais ferramentas poderiam lhe proporcionar a capacidade de agir de modo proativo diante de desafios e dilemas do cotidiano pertinentes à sua área de atuação.

Neste contexto, surgiram diversos questionamentos quanto à previsão e a reação diante de incidentes e problemas inerentes ao ambiente computacional de uma OM. De que forma pode-se monitorar a disponibilidade e o desempenho da uma infraestrutura de rede e suas aplicações?

A fim de melhor elucidar esta questão, o presente trabalho tem por objetivo abordar o assunto de maneira a apresentar a prática da instalação e configuração da ferramenta de software livre denominada Zabbix. Ferramenta esta capaz de agregar à área de TI poder de prevenção e reação à incidentes através do monitoramento da rede e de sistemas.

A solução desses desafios passa pelo estudo de ferramentas que possam aperfeiçoar o trabalho das equipes da área de TI.

A fim de adequar a resposta aos incidentes ocorridos em uma rede de computares estabelecida em uma organização, seja ela militar ou não. Surgiu a Ferramenta Zabbix.

Segundo Horst (2015), Zabbix é uma ferramenta moderna, de código aberto e multiplataforma, livre de custos de licenciamentos, utilizada para monitorar a disponibilidade e o desempenho de aplicações, ativos e serviços de rede por todo o mundo.

Este trabalho foi desenvolvido através da implementação de um servidor (gerente) Zabbix na rede de computadores do Comando de Operações Terrestres. Os agentes foram configurados nos serviços e servidores monitorados, e ainda, foram definidos gráficos e telas que pudessem ser estudados para uma posterior análise de resultados e conclusão de estudo.

2. REFERENCIAL TEÓRICO

2.1 Gerenciamento de Redes

Segundo Pinheiro (2006), o gerenciamento pode ser definido como coordenação, controle de atividade e monitoramento de recursos, assegurando na medida do possível confiabilidade, segurança e alta disponibilidade.

Atualmente as redes de computadores e os recursos associados, além das aplicações distribuídas, tem se tornado fundamental e de tal importância para uma organização, que elas basicamente não podem falhar (LIMA, 1997, p. 1).

De acordo com Saydam (1996), um sistema de gerenciamento de redes é constituído por quatro segmentos básicos sejam eles: o gerente, o agente, a base de informação gerenciada e os protocolos.

Ainda, segundo este autor, o gerenciamento de rede inclui o oferecimento, a integração e a coordenação de elementos hardware, software, além de pessoas para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos disponíveis.

Tanenbaum (2003) afirma que ativos são todos os componentes da rede que criam, processam, armazenam, transmitem ou descartam dados. Ainda segundo o autor, uma rede de computadores é uma infraestrutura de comunicação constituída

por um conjunto de equipamentos interconectados, a fim de trocar e compartilhar recursos e informações entre si e prover uma gama de serviços ao usuário.

Logo, equipamentos e serviços conectados à rede são passíveis de monitoramento, como por exemplo: servidores, *switches*, roteadores, impressoras, estações de trabalho, *nobreaks*, bem como os serviços de banco de dados e aplicações.

2.2 Protocolo TCP/IP

A fim de viabilizar a comunicação entre computadores padronizou-se a forma de iteração entre eles através de protocolos específicos que determinaram a forma e as regras de comunicação entre os mesmos.

O protocolo de comunicação de rede funciona como um idioma em que todos dispositivos que estão conectados à um ambiente específico têm a capacidade de receber e enviar informações.

De acordo com Forouzan (2008), o *Transmission Control Protocol - Internet Protocol* - TCP/IP é um conjunto de protocolos hierárquicos, compostos por módulos interativos, cada um dos quais provendo funcionalidades específicas. O termo hierárquico significa que cada protocolo de nível superior é suportado por um ou mais protocolos de nível inferior.

O protocolo TCP/IP é composto por quatro camadas, sejam elas: aplicação, transporte, rede e interface. Cada camada é responsável pela execução de tarefas específicas no transporte dos dados que trafegam pela rede.

2.3 *Management Information Base* - MIB

De acordo com Dias e Alves Junior (2001), um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas dos dados resultantes são os objetos gerenciados. Os objetos gerenciados podem ter permissões para serem lidos ou alterados, sendo que cada leitura representará o estado real do recurso e, cada alteração também será refletida no próprio recurso.

Dessa forma, a MIB é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede com uso baseado na pilha de protocolos TCP/IP.

Basicamente são definidos três tipos de MIBs: MIB II, MIB experimental, MIB privada.

A MIB II, que é considerada uma evolução da MIB I, fornece informações gerais de gerenciamento sobre um determinado equipamento gerenciado. Através das MIB II podemos obter informações como: número de pacotes transmitidos, estado da interface, entre outras.

A MIB experimental é aquela em que seus componentes (objetos) estão em fase de desenvolvimento e teste, em geral, eles fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.

MIB privada é aquela em que seus componentes fornecem informações específicas dos equipamentos gerenciados, como configuração, colisões e também é possível reinicializar, desabilitar uma ou mais portas de um roteador.

2.4 *Simple Network Management Protocol* – SNMP

De acordo com Dias e Alves Junior (2001), o SNMP é um protocolo de gerência definido em nível de aplicação, é utilizado para obter informações de servidores SNMP - agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP.

Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP – *User Datagram Protocol,* da pilha TCP/IP, para enviar e receber suas mensagens através da rede. Dentre as variáveis que podem ser requisitadas utilizaremos as MIBs podendo fazer parte da MIB II, da experimental ou da privada.

O gerenciamento da rede através do SNMP permite o acompanhamento simples e fácil do estado, em tempo real, da rede, podendo ser utilizado para gerenciar diferentes tipos de sistemas.

Este gerenciamento é conhecido como modelo de gerenciamento SNMP, ou simplesmente, gerenciamento SNMP. Por tanto, o SNMP é o nome do protocolo no

qual as informações são trocadas entre a MIB e a aplicação de gerência como também é o nome deste modelo de gerência.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objeto, de obtenção dos valores de um objeto e suas variações.

A utilização de um número limitado de operações, baseadas em um mecanismo de busca/alteração, torna o protocolo de fácil implementação, simples, estável e flexível. Como consequência reduz o tráfego de mensagens de gerenciamento através da rede e permite a introdução de novas características.

O funcionamento do SNMP é baseado em dois dispositivos o agente e o gerente. Cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual, estas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB.

2.5 Agente e Gerente

De acordo com Dias e Alves Junior (2001), o agente é um processo executado na máquina gerenciada, responsável pela manutenção das informações de gerência.

Principais funções de um agente:

- Atender as requisições enviadas pelo gerente; e
- Enviar automaticamente informações de gerenciamento ao gerente, quando previamente programado.

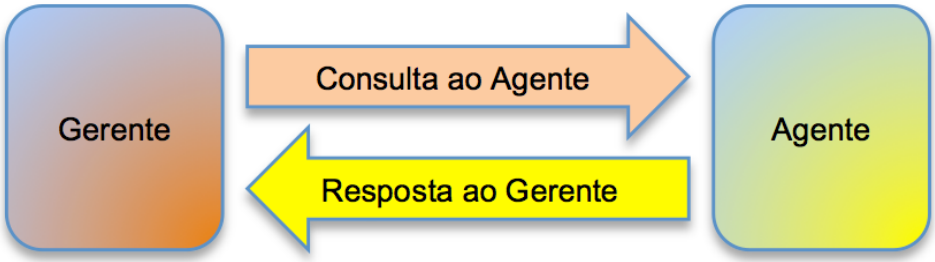
O agente utiliza as chamadas de sistema para realizar o monitoramento das informações da máquina e utiliza as RPC para o controle das informações da máquina.

Ainda segundo Dias e Alves Junior (2001), o gerente é um programa executado em uma estação servidora que permite a obtenção e o envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes.

O gerente fica responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas enquanto que o agente fica responsável pelas funções de

envio e alteração das informações e também pela notificação da ocorrência de eventos específicos ao gerente.

Figura 1 – Comunicação Gerente-Agente



Fonte: Elaborado pelo autor

2.6 Operações do protocolo SNMP

Segundo Dias e Alves Junior (2001), existem duas operações básicas (SET e GET) e suas derivações (GET-NEXT, TRAP).

A operação SET é utilizada para alterar o valor da variável; o gerente solicita que o agente faça uma alteração no valor da variável;

A operação GET é utilizada para ler o valor da variável; o gerente solicita que o agente obtenha o valor da variável;

A operação de GET-NEXT é utilizada para ler o valor da próxima variável; o gerente fornece o nome de uma variável e o cliente obtém o valor e o nome da próxima variável; também é utilizado para obter valores e nomes de variáveis de uma tabela de tamanho desconhecido;

A operação TRAP é utilizada para comunicar um evento; o agente comunica ao gerente o acontecimento de um evento, previamente determinado. São sete tipos básicos de TRAP determinados:

- *coldStart*: a entidade que a envia foi reinicializada, indicando que a configuração do agente ou a implementação pode ter sido alterada;

- *warmStart*: a entidade que a envia foi reinicializada, porém a configuração do agente e a implementação não foram alteradas;

- *linkDown*: o enlace de comunicação foi interrompido;

- *linkUp*: o enlace de comunicação foi estabelecido;

- *authenticationFailure*: o agente recebeu uma mensagem SNMP do gerente que não foi autenticada;

- *egpNeighborLoss*: um par EGP parou;
- *enterpriseSpecific*: indica a ocorrência de uma operação TRAP não básica.

2.7 A Ferramenta de Gerenciamento Zabbix

Zabbix é um software que monitora vários parâmetros de diversos ativos em uma rede de computadores. Possui uma interface gráfica extremamente agradável, com gráficos, mapas e telas muito bem desenvolvidas. É muito flexível e adaptado a monitorar praticamente todos os tipos de equipamentos e softwares, conforme cita Zabbix (2018).

O Zabbix foi criado por Alexei Vladishev em 1998. A ideia surgiu quando ele trabalhava em um banco na Letônia como administrador de sistemas, pois não estava satisfeito com as soluções de monitoramento que estava utilizando na época.

No Zabbix é possível definir regras para monitoramento e ações para solucionar alguns problemas. Desta forma, o software atua de maneira proativa resolvendo problemas automaticamente.

O sistema permite o envio de alertas via e-mail, SMS, Telegram, etc., além de contar com um efeito visual muito interessante, personalizável e intuitivo.

Segundo Lima (2014), o Zabbix possui a capacidade de monitorar milhares de itens em apenas um servidor, além de ser possível ter um monitoramento distribuído. Dessa forma, podemos ter um servidor central de monitoramento e vários outros servidores subordinados a ele enviando as métricas para o servidor central ou apenas replicar as informações. Também é possível separar os servidores web, servidor de banco de dados e servidor de monitoramento para aumentar a flexibilidade e ganhar em desempenho.

Ainda de acordo com Lima (2014), o Zabbix oferece um pacote completo, com mapas de rede, gráficos e telas, além de enviar alertas por e-mail ou SMS. Também pode executar ações, como, por exemplo, um comando remoto para recuperar um serviço sem a intervenção do administrador.

Corretamente configurado, ele pode desempenhar um papel importante no controle de uma infraestrutura, pois além de ser gratuito é fácil de ser implementado e gerenciável. Isto é igualmente verdade para as pequenas organizações com alguns servidores e para grandes empresas com um grande número de servidores.

Para maior capacidade de monitoramento, praticidade e vigor o software fornece ao administrador da rede um console central com monitoração em tempo

real e administração web, os monitores de desempenho incluem tudo, desde a memória do host, processador e espaço à utilização de swap em disco em todas as partições montadas, os processos em execução, os acessos a discos de leitura/gravação, *Proxy*, etc.

A principal funcionalidade dentre todas suas ferramentas é conseguir coletar informações de todos os dispositivos que estão interligados na rede, absorvendo as informações por meio de scripts, via agente ou até mesmo através do protocolo SNMP.

Segundo Lima (2014), o Zabbix integra todas as aplicações de que um sistema de gerenciamento de redes necessita, sem a necessidade de plug-ins, e é totalmente personalizável a qualquer tipo de ambiente.

Sua versão Server funciona em um servidor Linux, sendo compatível com diversas distribuições deste sistema operacional.

3. METODOLOGIA

Tartuce (2006) descreve que a metodologia científica é concebida no estudo sistemático e lógico dos métodos aplicados nas ciências, levando-se em conta seus fundamentos, sua validade e sua relação com as teorias científicas.

De forma geral, “[...] o método científico compreende basicamente um conjunto de dados iniciais e um sistema de operações ordenadas adequado para a formulação de conclusões, de acordo com certos objetivos predeterminados” (GERHARDT; SILVEIRA, 2009, p. 11).

A pesquisa exploratória, segundo Kerling (1973), possui três propósitos: descobrir variáveis significativas no campo alvo; descobrir a relação entre estas variáveis; formar a base para estudos posteriores mais aprofundados.

O presente trabalho caracteriza-se por ser uma pesquisa experimental e exploratória, de natureza aplicada, de abordagem quantitativa, do tipo estudo de caso. Para tal, realizou-se uma revisão teórica do assunto, através da pesquisa bibliográfica, documentos e trabalhos científicos (artigos, trabalhos de conclusão de curso, dissertações e teses).

Para alcançar este objetivo, baseado em Vergara (2005), dividiu-se o trabalho em etapas conforme descrito a seguir:

Inicialmente foi realizada revisão da literatura permitindo identificar as principais contribuições científicas sobre governança em TI, redes de computadores e o software Zabbix.

Posteriormente, elaborou-se análise bibliográfica sobre os termos abordados na pesquisa. O objetivo dessa etapa foi embasar as discussões realizadas posteriormente, visando à elaboração do documento acadêmico e o desenrolar das próximas etapas de pesquisa.

Em uma última etapa, realizou-se uma pesquisa experimental através de um estudo de caso, que possibilitou conhecer os procedimentos para o funcionamento do sistema.

Segundo Brodbeck (2001), as pesquisas recentes da área de TI, principalmente as com foco em planejamento e gestão, adotam métodos de estudo de caso. O método de estudo de caso vem sendo aplicado pela sociedade acadêmica, pois permite ter uma visão focada do problema que se quer pesquisar.

Segundo Merriam (1998), utiliza-se o estudo de caso quando se deseja compreender situações com uma maior profundidade, enfatizando seu significado para os vários problemas envolvidos.

Para a realização da análise quantitativa foi escolhido como ativo a ser monitorado e gerenciado o Servidor de Protocolo Eletrônico – SPED. O SPED trata-se de uma aplicação Web integrante do projeto Sistema Informatizado de Gestão Arquivística e Documental do Exército - SIGADEx.

O Projeto SIGADEx foi concebido para estabelecer a Governança Documental no âmbito do Exército, de forma a garantir o fluxo oportuno, preciso, seguro e confiável da informação na Força Terrestre.

Desta forma, o SPED é uma ferramenta utilizada amplamente em todos os níveis hierárquicos do Exército Brasileiro, por ser o sistema documental oficial da Força Terrestre.

Durante o processo de análise dos parâmetros do SPED foram mensurados e controlados os níveis de armazenamento, processamento e tráfego de redes.

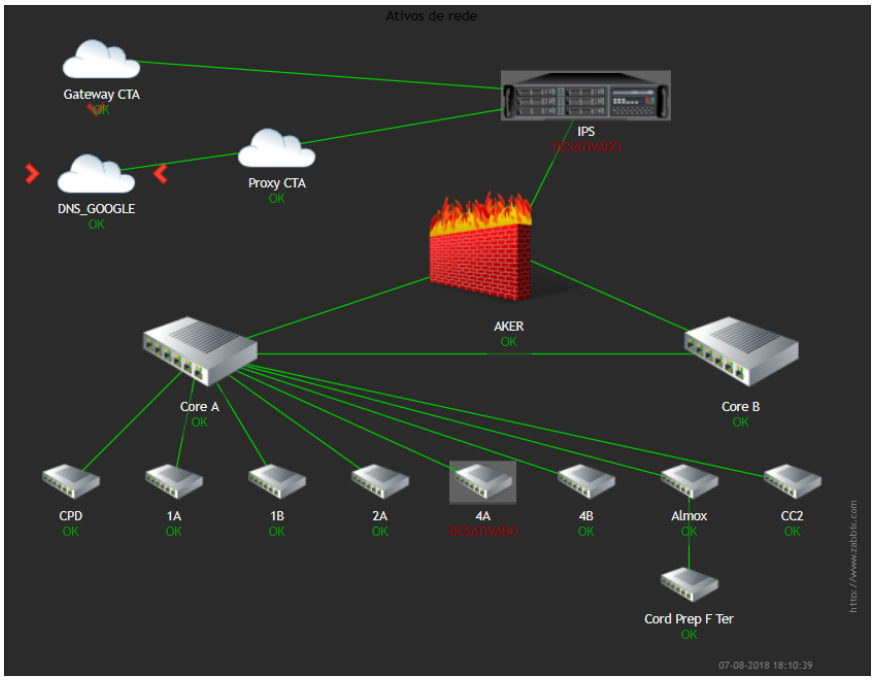
Além do SPED, foi monitorado o fluxo de dados do firewall de borda do COTER. Equipamento este de fabricação nacional produzido pela empresa AKER, por onde tramitam todas as informações digitais do ODOp.

4. RESULTADOS

O ambiente monitorado foi a rede de computadores do Comando de Operações Terrestres - COTER, Brasília-DF. A infraestrutura deste cenário é composta por computadores, servidores e *switches* interligados por uma estrutura física baseado no modelo Ethernet. A ligação entre os *switches* centrais (cores) e os *switches* de distribuição é estabelecida através de fibra óptica (Figura 2).

O servidor Zabbix (estação gerente) foi instalado em um servidor da Divisão de Informática do COTER, onde foram coletados os dados dos dispositivos da rede monitorada através do protocolo SNMP. Para atingir este objetivo foi necessário instalar um agente SNMP nos computadores monitorados. A instalação do servidor Zabbix e a configuração dos agentes estão disponíveis nos Apêndices A e B.

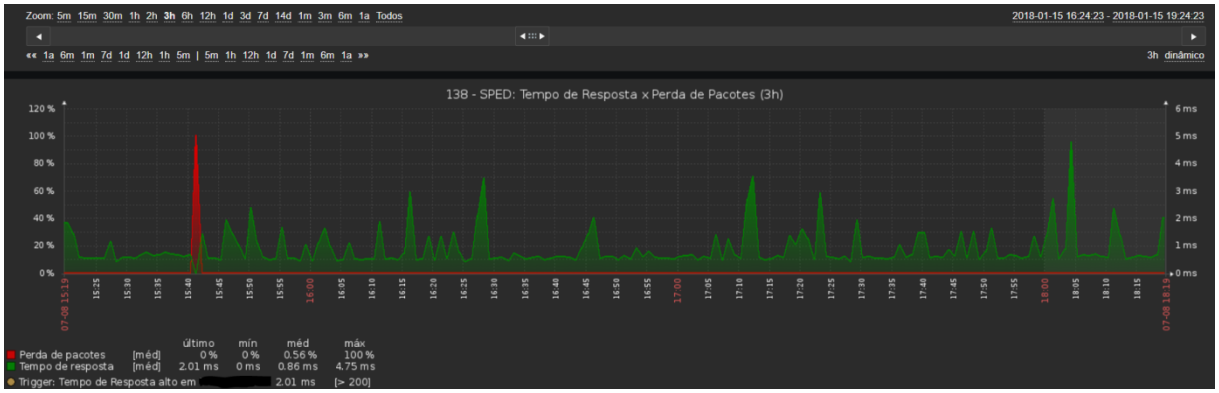
Figura 2 – Ativos de rede monitorados



Fonte: Elaborado pelo autor

O primeiro resultado é mostrado na Figura 3 e apresenta um gráfico mostrando o desempenho do tempo de resposta do servidor SPED na rede, contrapondo-se a quantidade dos pacotes de dados perdidos.

Figura 3 – SPED: Tempo de Resposta x Perda de Pacotes



Fonte: Elaborado pelo autor

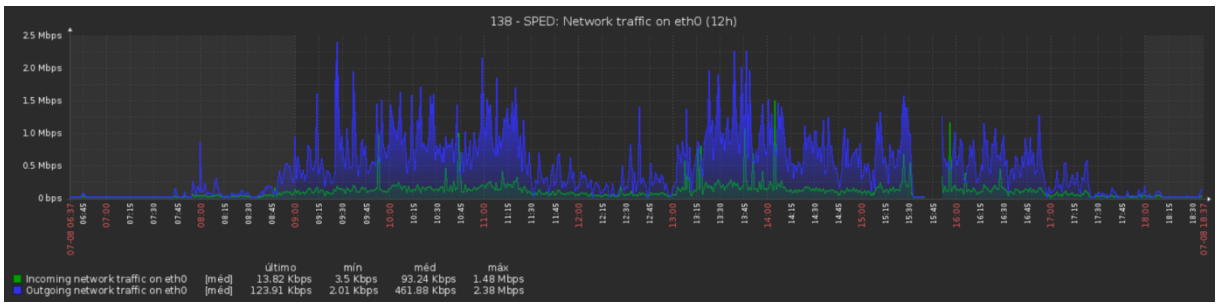
Observou-se que por volta das 15:40h houve uma interrupção de tráfego devido a desconexão de uma fibra óptica. Esta indisponibilidade foi indicada no gráfico pelo pico em cor vermelha na Figura 3, chegando ao percentual de 100% de perda de pacotes do servidor SPED coletadas pelo servidor Zabbix.

Verificou-se que a interrupção durou aproximadamente 3 minutos, quando houve o restabelecimento da conexão.

O tempo de resposta determina o período que o sistema leva para responder a uma entrada de usuário ou de um serviço. Um tempo de resposta muito alto pode indicar degradação do desempenho da rede, fazendo com que o usuário tenha que aguardar até que sua requisição seja processada. Na Figura 3 o tempo de resposta é medido em milissegundos.

Na Figura 3 pôde-se verificar que o tempo de resposta das requisições feitas pelo software Zabbix alcançou um tempo máximo de 4,75 ms (milissegundos) e uma média de 0,86 ms.

Figura 4 – SPED: Tráfego de Rede

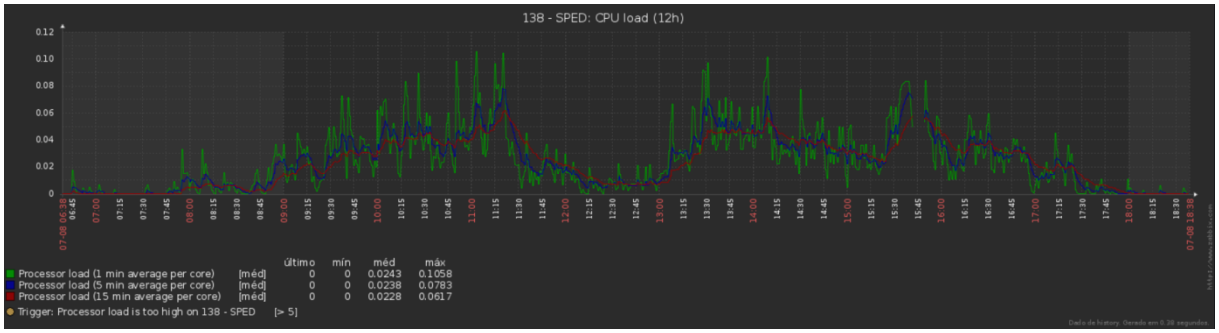


Fonte: Elaborado pelo autor

A Figura 4 forneceu a informação que o tráfego na interface de rede do servidor SPED foi interrompido por volta das 15:40h, tendo uma média de fluxo de entrada de dados de 93.24 kbps e de saída de 461.88 kbps.

Constatou-se na comparação da Figura 4 com a Figura 5 (Uso de CPU) que a indisponibilidade do servidor SPED foi causada pela interrupção do tráfego de dados e não por sobrecarga de processamento, pois a Figura 5 demonstrou que no momento em que o fluxo de rede foi cessado pelo incidente ocorrido, o Servidor SPED manteve seu processamento ativo, não apresentando no período verificado níveis de sobrecarga.

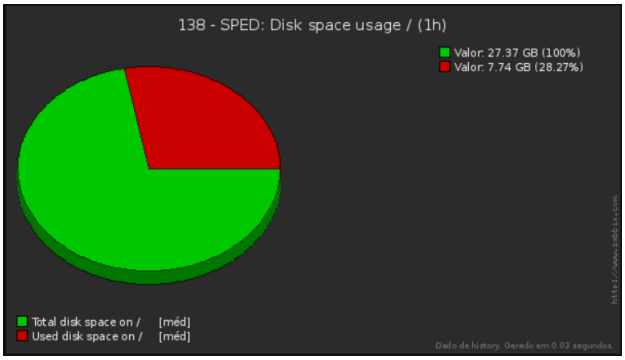
Figura 5 – SPED: Uso de CPU



Fonte: Elaborado pelo autor

A Figura 6 representa a capacidade de armazenamento do disco rígido do servidor SPED, bem como os percentuais de uso. Neste caso, o disco de tamanho de 27.37 Gb apresentou 7.74 Gb (28.27%) em Uso.

Figura 6 – SPED: Espaço em Disco

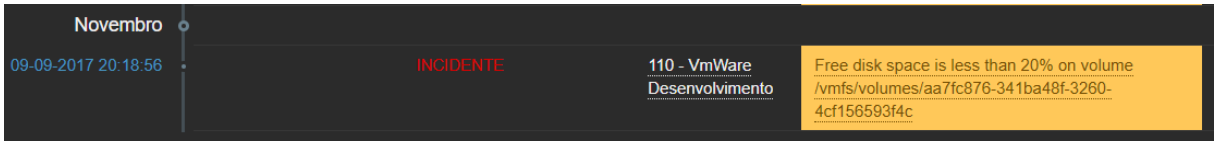


Fonte: Elaborado pelo autor

Este tipo de medição é crucial, pois permitiu configurar um gatilho (trigger) para quando o nível de uso do disco rígido chegar em 80%, por exemplo. Desta

forma, a equipe de TI recebe a informação através do painel de controle do Zabbix, podendo estabelecer procedimentos preventivos a uma provável saturação de espaço em disco, conforme visualizado na Figura 7.

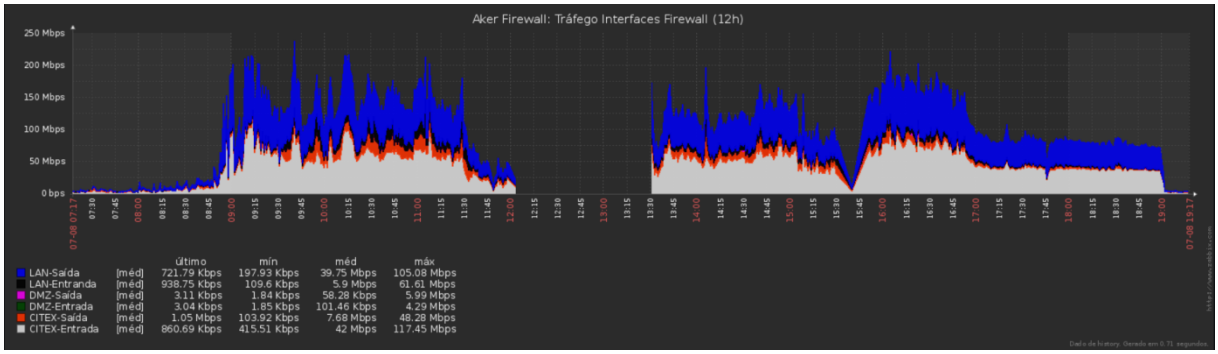
Figura 7 – Alerta: Espaço em Disco menor que 20%



Fonte: Elaborado pelo autor

A Figura 8 expõe o tráfego de rede das interfaces do firewall de borda. Onde ficou notório o incidente ocorrido no período de 12h a 13:30h. Neste lapso temporal este ativo de rede ficou desprovido de energia elétrica, desativando todo tráfego.

Figura 8 – Firewall: Tráfego de Rede



Fonte: Elaborado pelo autor

5. DISCUSSÃO

Utilizando informações mais detalhadas sobre os ativos de redes do COTER, as ações de suporte ao usuário deixaram de ser apenas reativas, passando a ser proativas. Esta mudança ocorreu devido ao aumento na disponibilidade de informações, que permitem à equipe de suporte ter conhecimento sobre o problema muitas vezes antes mesmo dos usuários o perceberem. Estas informações permitiram reduzir os deslocamentos *in loco* para verificação das ocorrências, bem como ajustar a configuração dos ativos para adequar as novas necessidades.

Outro resultado de impacto foi o aumento da diversificação dos alertas de eventos ocorridos. Os alertas puderam ser diversificados para painéis de controle

personalizados com alertas para grupos específicos de ativos e o envio de *e-mail* dos eventos ocorridos para a equipe de suporte.

Apesar das vantagens apresentadas, o fato que dificulta a utilização do *Zabbix* é a criação dos modelos (*templates)* a serem utilizados para monitorar os ativos de rede. Devem ser criados manualmente e adicionados aos ativos de redes compatíveis, no caso de incompatibilidade entre eles, novos modelos devem ser criados.

Neste caso para criar um modelo é necessário criar o item, o gráfico e o gatilho *(trigger)*, e dependendo da quantidade de itens a ser adicionada ao modelo, sua criação se torna muito trabalhosa.

6. CONCLUSÃO

O presente trabalho apresentou uma proposta de implementação de uma solução de gerência de redes de computadores no ambiente do COTER usando a ferramenta de monitoramento Zabbix.

Comprovou-se a eficácia na utilização do Zabbix como ferramenta de apoio ao monitoramento de ativos de rede, bem como na viabilização de poder de reação da equipe de TI diante de dilemas e incidentes futuros, oferecendo a capacidade de execução de medidas e procedimentos pertinentes de forma proativa.

Durante o período de implementação foram coletados dados de ativos com a finalidade de analisar o desempenho da rede de computadores Comando de Operações Terrestres.

Os dados coletados pelo software Zabbix foram mostrados em gráficos possibilitando a análise de parâmetros relevantes ao desempenho da rede monitorada.

Os gráficos foram gerados em tempo real o que proporcionou um acompanhamento mais eficaz e maior rapidez nas decisões tomadas pelo gerente da rede.

Com os resultados obtidos pôde-se observar aspectos que podem servir de subsídios para o planejamento e expansão dos serviços ofertados.

O monitoramento de armazenamento demonstrou-se eficaz, pois possibilitou a identificação de uma possível falta dos recursos em disco rígido.

O monitoramento do servidor SPED agregou conhecimento no gerenciamento de um serviço amplamente utilizado pelo Exército Brasileiro. Trazendo consigo ensinamentos conhecidos na caserna como “Lições Aprendidas” que podem ser replicados e multiplicados no âmbito da Força Terrestre, evitando desta forma, o retrabalho na configuração de monitoramento desta aplicação.

Logo, a implementação do Zabbix como ferramenta de monitoramento do SPED, demonstrou-se útil, viável e oportuna, pois proporcionou a equipe de TI do COTER informações e métricas exatas de utilização de tempo de resposta do serviço, consumo de CPU, medição do tráfego de rede e espaço em disco, conforme apresentado pelas Figuras 1 a 6 deste trabalho. Além disso, a ferramenta disponibiliza a preparação de gatilhos em função de determinada condição expressa no Zabbix, como por exemplo, o monitoramento da disponibilidade do disco rígido.

Através da análise dos gráficos e configurações de gatilhos, o Zabbix, permitiu que medidas proativas e corretivas fossem adotadas em um espaço de tempo menor quando comparado a uma gestão sem monitoramento, pois nesta, a busca pela origem dos incidentes torna-se mais um passo da solução do problema.

Diante ao exposto, o Zabbix demonstrou-se como uma opção consistente de gerenciamento de um parque computacional, pois oferece a consciência situacional do ambiente monitorado para a equipe de TI responsável, propiciando a oportunidade de tomadas de atitudes preventivas e corretivas para a manutenção da estabilidade de todo sistema.

Nesse contexto como sugestão para trabalhos futuros podem ser realizados o gerenciamento de redes com ênfase na segurança, onde viabiliza-se o monitoramento de vulnerabilidades de sistemas e infraestruturas sensíveis.

REFERÊNCIAS

BRODBECK, A. F. **Alinhamento estratégico entre os planos de negócios e de tecnologia de informação: um modelo operacional para a implantação**. 2001. Tese (Doutorado em Administração) - Programa de Pós-graduação em Administração da Universidade Federal do Rio Grande do Sul, Porto Alegre, 2001.

DIAS, B. Z.; ALVES JUNIOR, N. **Protocolo de gerenciamento SNMP**. 2001. Disponível em: <http://www.rederio.br/downloads/pdf/nt00601.pdf>. Acesso em: 11 jul. 2018.

FOROUZAN, Behrouz A.; FEGAN, Sophia Chung. **Protocolo TCP/IP**. 3. ed. São Paulo: Mcgraw-hill, 2008. p. 864.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de Pesquisa**. Porto Alegre: Editora da UFRGS, 2009.

HORST, A. H. S; PIRES, A. S; DÉO, A. L. B. **De A a ZABBIX**. 1.ed. São Paulo: Novatec Editora Ltda., fev. 2015.

KIELING, R. C. **A Viabilidade de Projetos em TI Alinhada ao Planejamento Estratégico das Empresas**. 2005.

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

MERRIAM, S.B. Q**ualitative Research and Case Study Applications in Education**. San Francisco: Allyn and Bacon, 1998.

PINHEIRO, J. M. S. **Gerenciamento de Redes de Computadores**: Uma Breve Introdução. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php>. Acesso em: 11 jul. 2018.

SAYDAM, T.; MAGENDAZ, T. **From networks and network Management into Service Management** - Journal of Networks and Systems Management, vol.4, n. 4, dez 1996, p. 345-348.

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

TARTUCE, T. J. A. **Métodos de pesquisa**. Fortaleza-CE: UNICE, 2006.

VERGARA, S. C. **Métodos de Pesquisa em Administração**. São Paulo: Atlas, 2005.

ZABBIX. **The Enterprise-class Monitoring Solution for Everyone**. Zabbix SIA. Disponível em: <http://www.zabbix.com/about.php>. Acesso em: 11 de jul. 2018.

APÊNDICE A – INSTALAÇÃO DO SERVIDOR ZABBIX

wget http://repo.zabbix.com/zabbix/3.2/debian/pool/main/z/zabbix-release/zabbix-release_3.2-1+jessie_all.deb

dpkg -i zabbix-release_3.2-1+jessie_all.deb

apt-get update

apt-get install zabbix-server-mysql zabbix-frontend-php

Instalando o agente:
apt-get install zabbix-agent

Criação do Banco de Dados:

shell> mysql -uroot -p
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by '<SENHA DO BANCO DE DADOS>';
mysql> quit;

Importação inicial de schemas e dados:

cd /usr/share/doc/zabbix-server-mysql
zcat create.sql.gz | mysql -uroot zabbix

Editando configuração do zabbix server em zabbix_server.conf:

vim /etc/zabbix/zabbix_server.conf

DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbix

Start no Zabbix server:

service zabbix-server start

Start no Apache server:

service apache2 restart

APÊNDICE B – ATIVAÇÃO AGENTE DO ZABBIX NOS SERVIDORES LINUX

Instalar pacotes necessários:

apt-get install zabbix-agent

Fazer cópia de arquivo de configuração original:

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

Criar novo arquivo de configuração:

touch /etc/zabbix/zabbix_agentd.conf

Inserir o conteúdo 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

Restartar o serviço do zabbix agente:

service zabbix-agent stop

service zabbix-agent start

Caso seja necessário liberar o agente do zabbix no firewall:

iptables -A INPUT -p udp --dport 10050 -j ACCEPT
iptables -A FORWARD -p udp --dport 10050 -j ACCEPT
iptables -A INPUT -p tcp --dport 10050 -j ACCEPT
iptables -A FORWARD -p tcp --dport 10050 -j ACCEPT
iptables -A INPUT -p udp --dport 10051 -j ACCEPT
iptables -A FORWARD -p udp --dport 10051 -j ACCEPT
iptables -A INPUT -p tcp --dport 10051 -j ACCEPT
iptables -A FORWARD -p tcp --dport 10051 -j ACCEPT