

Zabbix Monitoramento Distribuído em Central de Operações de Redes

Rodrigo de Avila Dotto¹, Walter Priesnitz Filho²

¹Tecnologia em Redes de Computadores – Universidade Federal de Santa Maria Rio Grande do Sul (UFSM)
Cep – 97.105-900 – Santa Maria – RS – Brasil

²Tecnologia em Redes de Computadores – Universidade Federal de Santa Maria Rio Grande do Sul (UFSM)
Cep – 97.105-900 – Santa Maria – RS – Brasil.

rodrigo.dotto@redes.ufsm.br, walter@redes.ufsm.br

Abstract. *This article presents a case study, where the goal is to deploy network management in small businesses. From this, present the possibility of developing a network operations center focused on monitoring with Zabbix..*

Resumo. *Este artigo trata de um estudo de caso, onde o objetivo é implantar gerenciamento de redes em empresas de pequeno porte. A partir deste apresentar a possibilidade do desenvolvimento de um centro de operações de rede com foco em monitoramento com Zabbix .*

1. Introdução

As redes de computadores passaram a ser vital para o funcionamento de muitas organizações. Com isso, emerge a necessidade de um suporte adequado para manter a disponibilidade e a confiabilidade dos sistemas computacionais. Muitas vezes o custo com técnicos para manter um monitoramento local em pequenas empresas não se justifica, diante desta realidade surge como alternativa a terceirização deste serviço. Surge então a oportunidade de implantar um NOC (Centro de operação de redes). Como objetivo deste estudo, projeta-se de forma compartilhado, escalável, utilizando uma ferramenta Open Source.

A ferramenta Zabbix se apresentou com grande candidata no desenvolvimento deste estudo de caso, por ser Open Source e oferecer suporte a monitoramento distribuído. A fim de contribuir para a comunidade acadêmica e ajudar positivamente a desenvolver uma solução no gerenciamento de rede de pequenas empresas desenvolve-se este projeto de pesquisa aplicando-o em um cenário real.

2. Referencial Teórico

Tendo conhecimento da fragilidade computacional necessita-se buscar meios de antecipar e ou minimizar os possíveis danos, sendo assim pode-se prever possíveis problemas e diminuir o tempo de reparo. Desta forma, as ferramentas de monitoramento têm potenciais a fim de contribuir com a continuidade do negócio das empresas (VALE, 2017). Uma rede sem gerenciamento está em risco eminente, tanto na falta de previsão de possíveis problemas, quanto para solucionar uma ocorrência.

A partir destas necessidades, iniciou-se há muito tempo pesquisas sobre gerenciamento de redes conforme afirma Pinheiro (2002,p4). E estudo de passou a pesquisar sobre os benefícios, implantação e monitoramento de redes utilizando-se da ferramenta Zabbix. O Zabbix é uma ferramenta bastante flexível, de classe *enterprise*, capaz de monitorar qualquer coisa. pode ser utilizada em um único servidor, mas também permite que seja implementada em uma estrutura de monitoramento distribuída, coletando informações de diversos locais e concentrando tudo em um único banco de dados (VALE, 2015).

Manter uma rede de computacional sob gerenciamento constante se tornou uma necessidade para as organizações, pouco tempo dos serviços indisponíveis trazem muitos prejuízos, nem sempre só financeiros, é preciso amenizar e ou antecipar os problemas possíveis.

3. Metodologia

Desta forma, este trabalho foi desenvolvido em três etapas: a primeira consistiu em pesquisas bibliográficas, a segunda foi aplicação em laboratório, e a terceira consistiu na implantação em cenário real. Todos os processos foram fundamentais para o esta pesquisa, uma vez que o entendimento teórico do assunto contribuiu para suprimir os desafios da prática.

Devido aos riscos na implantação da ferramenta de gerenciamento a empresa parceira (cenário real), se tornou de vital importância a implantação em laboratório. No estudo em laboratório não existe o interesse de analisar os dados coletados, o principal objetivo era levantar a utilização de recursos de hardware para o funcionamento do sistema (*Zabbix Server, Agent e Proxy*).

A implantação em laboratório ocorreu da seguinte forma: Instalação do Zabbix *Server* em um computador com a seguinte configuração: processador de um núcleo Intel Atom 1.6GHz, memória 900Mb e disco rígido de 4GB e sistema operacional Linux Ubuntu Server 16.04. Durante o estudo de laboratório utilizou-se três equipamentos com o Zabbix *Agent*, dois equipamentos com sistema operacional Windows® *Seven* e outro equipamento Linux Ubuntu Server 16.04.

A implantação em laboratório seguiu para a próxima etapa, a implantação do Zabbix *Proxy* efetuado em uma máquina virtual (configuração de hardware idêntica à utilizada para o Zabbix *Server*). Após a implantação bem sucedida em laboratório de um cenário similar ao real, onde o Zabbix *Proxy* coletava os dados dos três equipamentos com Zabbix *Agent* e repassava para o Zabbix *Server*, analisando a utilização de recursos do Zabbix *Proxy* (que ficará instalado no cliente) conclui-se não traria nenhum impacto para o funcionamento da rede na empresa parceira, sendo assim partimos para implantação no cenário real.

A loja parceira, é uma empresa varejista que disponibiliza mais de cinco mil itens para comércio, o seu parque de máquinas de informática consiste de um servidor com sistema operacional Windows® Server 2012, seis computadores caixa, sete computadores do setor administrativo, quatro computadores para consulta de preços, quatro equipamentos busca preços, um DVR, um ponto eletrônico, duas impressoras IP, um *switch* 10/100/1000 24 portas, um *switch* 10/100 16 portas e dois modems ADSL (Linha Digital Assimétrica para Assinante).

A implantação: No servidor da empresa (Windows Server 2012) foi instalada uma máquina virtual (Virtualbox) com sistema operacional Linux Ubuntu Server 16.04 onde está instalado Zabbix *Proxy*. Foi instalado o Zabbix *Agent* em 19 computadores e outros oito equipamentos (busca preços, ponto, impressoras, DVR) efetuado somente teste de disponibilidade. Os computadores com Zabbix *Agent* monitora-se: utilização o disco rígido, utilização de memória física, tráfego de dados das placas de rede, consumo de processamento e um serviço de backup.

Remotamente, o cenário conta com o servidor proposto para a NOC, com outra máquina virtual com o Virtualbox, também com sistema operacional Linux Ubuntu Server 16.04 e o Zabbix *Server* para o recebimento dos dados, tratamento e análise das informações.

4. Resultados

Os resultados etapas um e dois deste estudo de caso foram obtidos com sucesso. A etapa três mesmo estando em desenvolvimento e aprimoramento já apresenta resultados interessantes.

4.1. Primeira Etapa

Neste estudo de caso se observa a aplicação da teoria sobre redes de computadores, onde a empresa compartilha um banco de dados com todos os setores, administrativo (lançamento de notas, vendas em grande volume, reposição mercadorias, ...), vendas balcão (caixas com grande volume de itens), consulta de preços (equipamentos busca preços), compartilhamento de impressoras IP, entre outros equipamentos para o bom funcionamento da empresa.

A partir do entendimento do funcionamento da rede de computadores, da ferramenta Zabbix e dos seus benefícios, seguiu-se a etapa prática de testes em laboratório.

4.2. Implantação em Laboratório

Nesta fase os principais objetivos foram efetuar a implantação do Zabbix *Server*, Zabbix *Agent* em equipamento com sistema operacional Linux e Windows e por fim a implantação do Zabbix *Proxy* seja possível desenvolver um NOC para monitoramento da rede de pequenas empresas.

No Zabbix *Server*, três pontos fundamentais foram observados em laboratório: o tráfego de rede, a utilização de memória RAM e disco rígido, e o consumo de processador. Essa análise se torna de grande importância uma vez que mede os impactos causados pela ferramenta (Zabbix) para que a implantação na empresa parceira não resulte em transtornos. Na etapa um não se encontram informações precisas sobre quais configurações de hardware são necessárias para monitorar um número n de equipamentos, mesmo que apresentados na literatura, dificilmente se encontra os dados de um cenário real e sim o recomendável. Em busca dessas informações utilizou-se de um equipamento de baixa configuração para o Zabbix *Server* foi implantado em uma máquina virtual Virtualbox com processador Intel Atom 1.6Ghz, 800Mb de memória ram e 4GB de disco rígido.

A implantação em laboratório foi muito bem sucedida e surpreendente, mesmo com uma configuração de hardware modesta, em nenhum momento o Zabbix Server apresentou baixo desempenho ao monitorar a rede com três equipamentos. Observa-se o baixo tráfego de rede (Figura 1), pois os pacotes recebidos dos *Agents* são pequenos, uma média de 1.54Kbps de envio e 1.9Kbps recebimento.

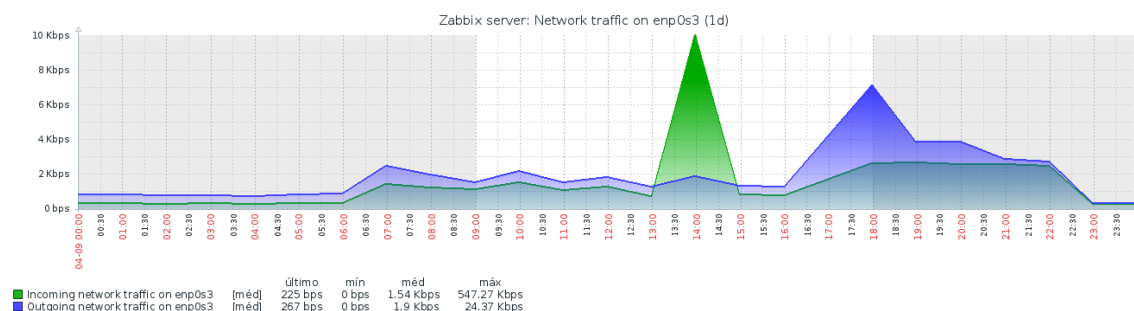


Figure 1. Tráfego de dados porta enp0s3 Zabbix Server, data 04.09.2018.

A utilização de memória da máquina virtual com Zabbix *Server* manteve-se estável (Figura 2), utilizando apenas 500MB em média.

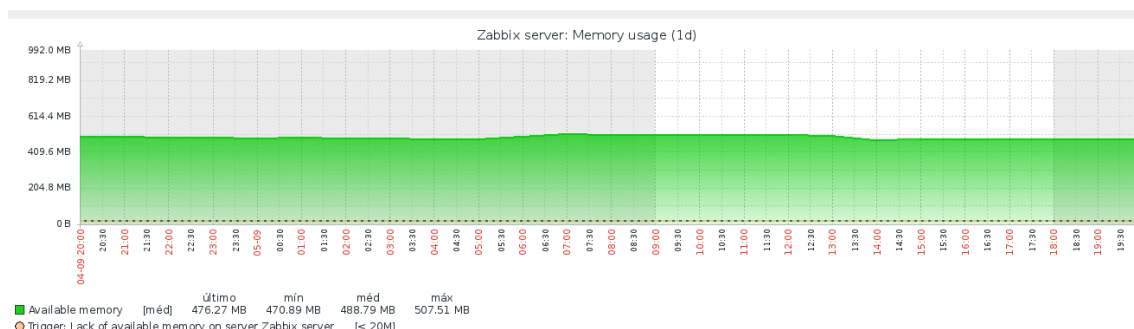


Figure 2. Utilização memória no Zabbix Server, data 04.09.2018.

O mesmo ocorreu com o espaço em disco (Figura 3), mantendo uma média de 86% do espaço livre, o banco de dados obteve um crescimento mínimo da data inicial ao término dos testes.

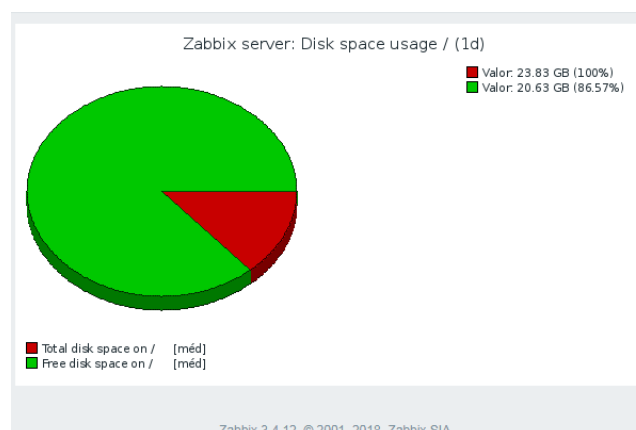


Figure 3. Utilização disco rígido no Zabbix Server, data 04.09.2018.

Com relação ao processamento, o desempenho foi ainda melhor (Figura 4), processador teve uma média de 98% do processador disponível.

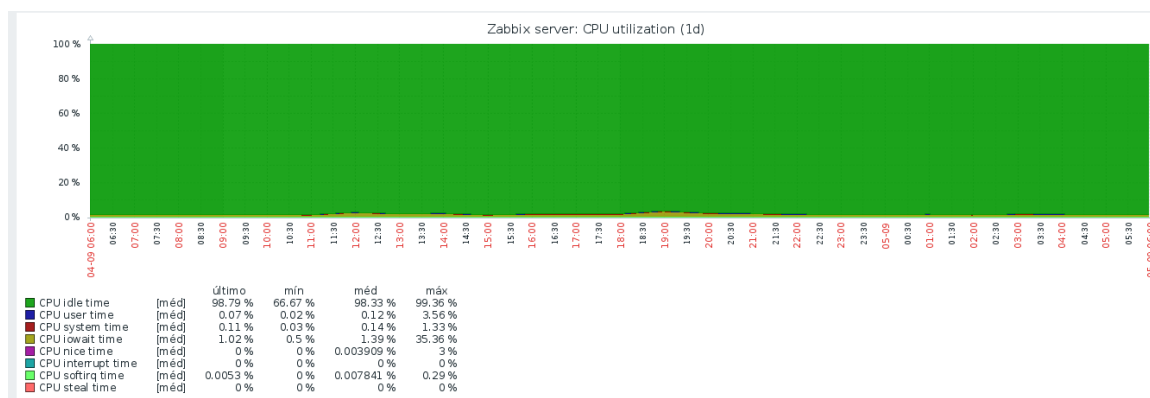


Figure 4. Consumo de processamento no Zabbix Server, data 04.09.2018.

A implantação do Zabbix *Agent* nos equipamentos foi bem sucedida. A expectativa era maior quanto a implantação do Zabbix *Proxy*, já que adiciona uma camada adicional ao sistema de coleta de informações de gerenciamento. A implantação do Zabbix *Proxy* utilizou uma máquina virtual idêntica à utilizada no Zabbix *Server*. As configurações dos *Agents* foram alteradas para que os dados fossem enviados para o Zabbix *Proxy* e o Zabbix *Proxy* ficou responsável em enviar para o Zabbix *Server*. Esta etapa ganhou um ingrediente interessante pois o Zabbix *Proxy* envia os dados para o servidor por um endereço DDNS (Dynamic Domain Name System) já que a localização do Zabbix *Server* não possui IP público fixo.

O Zabbix *Proxy* foi configurado inicialmente para manter os dados dos *Agents* por 24h em caso de perda de comunicação com o Zabbix *Server*. Logo existe a necessidade de monitorar o Zabbix *Proxy*. Observa-se que a utilização de recursos do Zabbix *Proxy* é ainda menor que a utilização do Zabbix *Server*, tráfego de rede (Figura 5), utilização de memória (Figura 6), processamento (Figura 7).

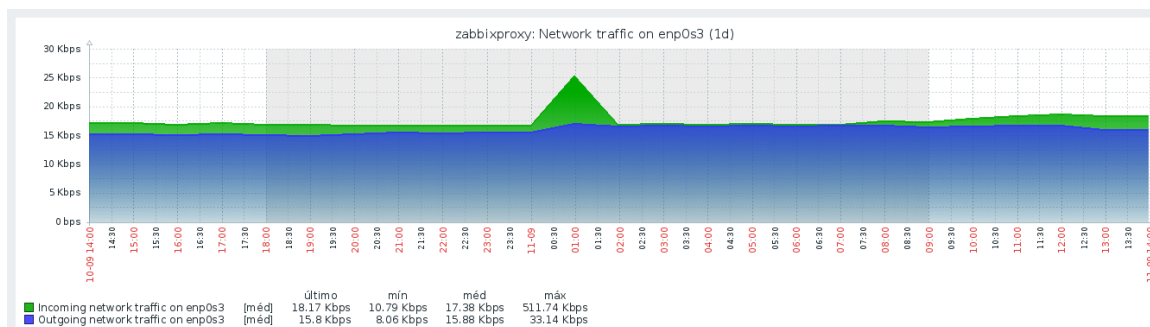


Figure 5. Tráfego dados porta enp0s3 no Zabbix Proxy, data 10.09.2018.

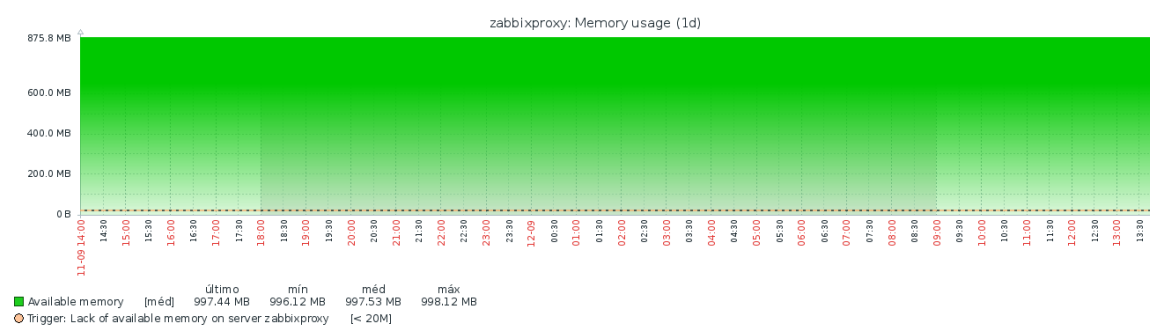


Figure 6. Utilização memória no Zabbix Proxy, data 10.09.2018.

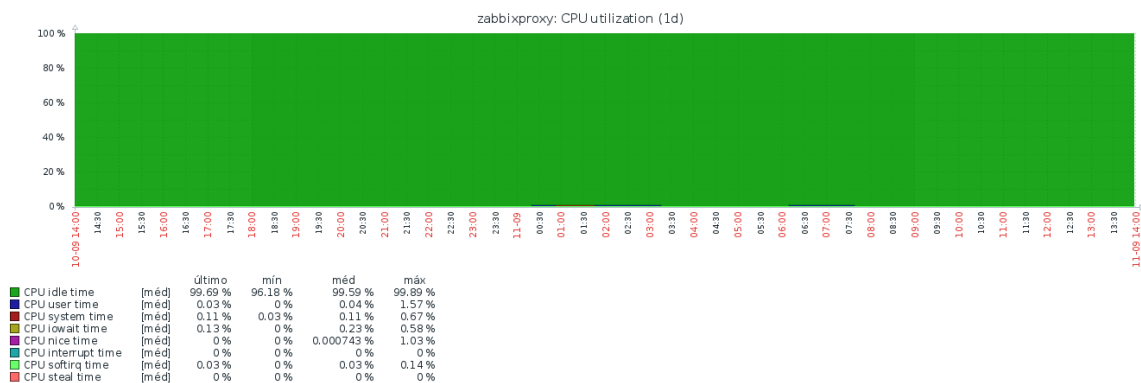


Figure 7. Processamento no Zabbix Proxy, 99,5% livre data 04.09.2018.

Notou-se que o Zabbix necessita de poucos recursos computacionais para gerenciar recursos como os que o ambiente proposto requer: tráfego de rede, memória, disco rígido e processamento. Desta forma se apresenta adequado para a implantação no cenário real sem impactar na infraestrutura da empresa..

4.2. Implantação em cenário real, disponibilizado por empresa parceira.

Os maiores desafios desta etapa se apresentaram na implantação do Zabbix *Proxy*, que envia os dados ao Zabbix *Server* em laboratório remoto, e implantação do Zabbix *Agent* sem causar impacto no funcionamento da empresa. Outra questão importante que foi levado em conta, foi o efeito psicológico no qual qualquer problema ocorrido a partir da implantação pudesse levar os usuários a associar o problema com o sistema de monitoramento. Portanto se estabeleceu que a empresa seria informada da data de implantação. A implantação em todos os equipamentos ocorreu na data de 19.10.2018 e está em monitoramento para levantamento de dados e comparações.

A implantação do Zabbix *Proxy* foi um sucesso, o Zabbix *Server* recebe os dados (Figura 8), trata e disponibiliza as visualizações no *dashboard* que pode ser acessado remotamente de qualquer ponto da Internet, atualmente monitora 28 hosts remotos e 2906 itens. Discute-se a seguir alguns resultados relevantes.

Nome	Modo	Criptografia	Visto pela última vez (tempo)	Contagem de hosts	Contagem de itens	Performance requerida (vps)	Hosts
zabbixproxy	Ativo	NENHUM	0	28	2906	46.23	BUSCA PRECO01 ENTRADA, BUSCA PRECO02 LADO, BUSCA PRECO03 MEIO, BUSCA PRECO04 FUNDOS, CAIXA01, CAIXA02, CAIXA03, CAIXA04, CAIXA05, CAIXA06, CLAUDIA-PC, CLIP_NOTAS, CONSULTA ENTRADA, CONSULTA FUNDOS, CONSULTA LADO, DANIEL-PC, DVR, ESTIQUETAS, ESTOQUE, EUNICE-PC, IMPRESSORA FRENTE, IMPRESSORA FUNDOS, MODEM, PAULO-PC, PONTO, RAFAEL-PC, SERVER_CLIP, zabbixproxy

Figure 8. Dados recebidos do Zabbix Proxy, data 08.10.2018.

Exibem-se as alterações de comportamento do Zabbix *Server* e Zabbix *Proxy* ao receber um maior número de dados para tratamento. No Zabbix *Server* o tempo de processamento livre em média caiu de 98% para 95%, o espaço em disco livre diminuiu de quanto? para 80% livre, a utilização de memória pouco aumentou em média disponibiliza 365MB livre e o destaque foi para utilização do tráfego de dados entre Zabbix *Server* e Zabbix *Proxy* que aumentou consideravelmente (Figura 9) de uma média de 1.56Kbps de envio e 1.9Kbps recebimento em laboratório para 21.19Kbps envio e 59.96Kbps recebimento, dados coletados na data de 08.10.2018.

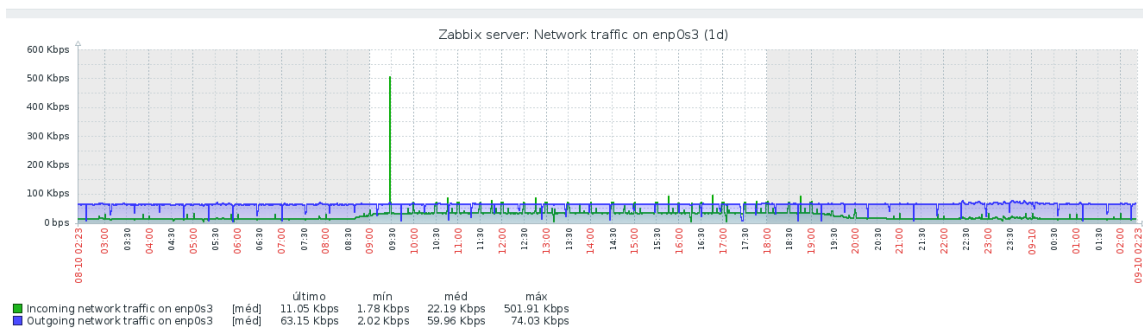


Figure 9. Tráfego de dados porta enp0s3 Zabbix Server, data 08.10.2018.

Um fato relevante que poderá trazer benefícios a empresa parceira, foi a observação de tráfego de dados anormal em dois computadores da administração, enquanto cinco dos sete computadores enviam uma média de dados inferior a 1Mbps (Figura 10), outros dois equipamentos tem média superior a 4Mbps (Figura 11). O computador que apresentou esse elevado tráfego de dados é responsável pela análise das filmagens do sistema de câmeras, assim se justificou essa elevada utilização.

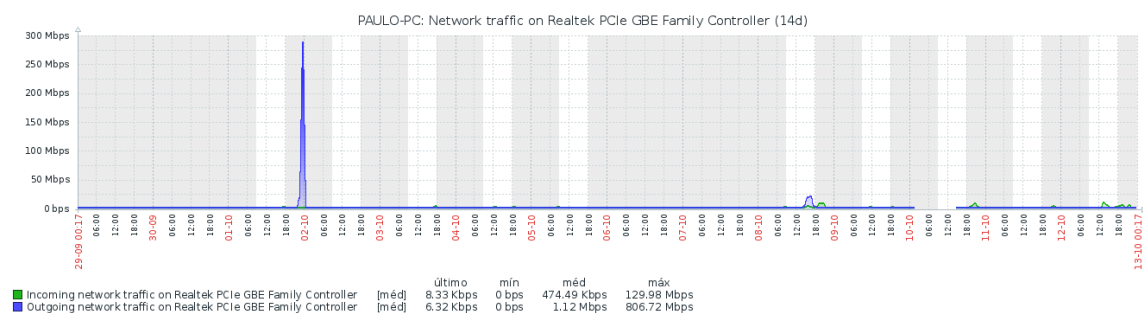


Figure 10. Tráfego de dados normal setor administrativo.

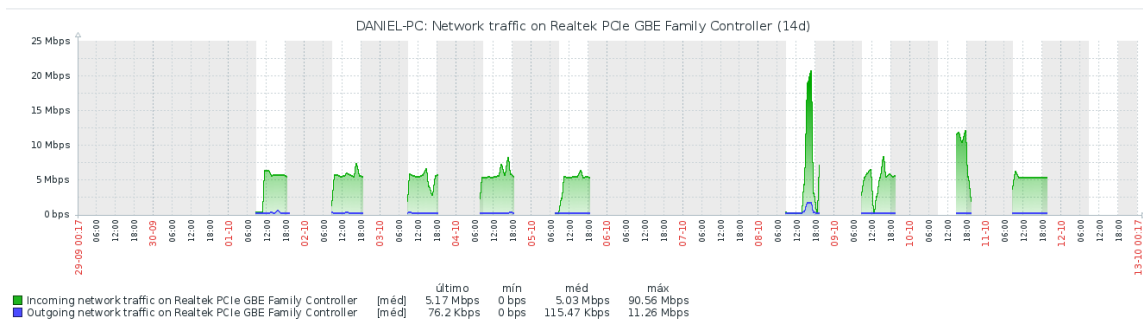


Figure 11. Tráfego de dados anormal setor administrativo.

Outros resultados importantes já foram observados, efetuando um comparativo de ocorrências relatadas pela empresa com os registros do monitoramento se detectou uma boa eficiência da ferramenta Zabbix.

5. Conclusões

Este estudo de caso segue no caminho de efetuar ajustes finos nos alertas, gatilhos de ocorrências, e implantação em mais empresas para a real montagem de um centro de operações de rede NOC.

A partir deste estudo de caso, conclui-se que a utilização da ferramenta Zabbix é uma poderosa aliada quando o assunto é gerenciamento de redes. Neste trabalho se constata o baixo consumo de recurso computacional na implantação do Zabbix *Server* e Zabbix *Proxy*, a facilidade de trabalhar no *dashboard*, a agilidade de transmissão, recebimento e tratamento dos dados com uma utilização insignificante da rede e por ser um sistema Open Source. Portanto se torna muito atraente a implantação de um NOC para efetuar o monitoramento de várias empresas de pequeno porte em um ponto centralizado NOC, contribuindo assim para o bom funcionamento da rede das empresas monitoradas.

6. Desafio

Estudo aprofundado dos protocolos de gerenciamento;

Gerenciamento de dispositivos móveis;

Criação de um *Template* enxuto “universal”;

Estudo e comparação com outras ferramentas;

Aplicação de software como serviço?

6. Referências

- Benício, Washington. Monitoramento e Gerenciamento de Redes Utilizando Zabbix. 2015.
- Brasil, Zabbix. Disponível em: < <http://zabbixbrasil.org/> >. Acesso em: 09 ago. 2018.
- Júnior, Valter Lisbôa. Soluções de Monitoramento com Zabbix. 4Linux Free Software Solutions.
- Lima, Janssen dos Reis. Monitoramento de Redes com Zabbix. Rio de Janeiro: Brasport 2014.
- Neto, Arlindo; Uchôa, Joaquim. Ferramentas Livres para Monitoração de Servidores. Fisl 7.0.
- Scapin, Alex. Análise de Ferramentas de Gerencia de Redes e Interfaces Web, 2015.
- Vale, André. A Importância do Monitoramento de Redes para a Segurança da Informação. 2017.
- Vale, André Luiz Mariano do. Monitoramento de redes: a importância do monitoramento de redes para a segurança da informação. Monografia, 29p. Universidade do Sul de Santa Catarina, 2017. Disponível em: < <https://riuni.unisul.br/handle/12345/4661> >. Acesso em: 10 ago. 2018.