HOLOS

ISSN: 1518-1634

holos@ifrn.edu.br

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Brasil

SILVA, W.M.C.; MEDEIROS, R.M.; MARTINS, R.S.

ANÁLISE E GERENCIAMENTO DE REDES USANDO UMA METODOLOGIA PROATIVA COM ZABBIX

HOLOS, vol. 8, 2015, pp. 277-289

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Natal, Brasil

HOLOS
ISSN 1807 - 1600

# ANÁLISE E GERENCIAMENTO DE REDES USANDO UMA METODOLOGIA PROATIVA COM ZABBIX

**W. M. C. SILVA[*], R. M. MEDEIROS e R. S. MARTINS**
[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
wanderson.michel.cs@gmail.com[*]

Artigo submetido em setembro/2014 e aceito em dezembro/2015

DOI: 10.15628/holos.2015.2441

## RESUMO

Diante do crescimento de empresas que adotam a tecnologia da informação como ferramenta estratégica e de controle, o gerenciamento de redes surge como necessidade em um ambiente que o número de dispositivos de redes aumenta com o decorrer do tempo. Visando a centralização da gerência de redes e o baixo custo para implementação, esse artigo propõe a utilização da ferramenta Zabbix e do protocolo SNMP, não somente para monitoramento e controle, mas para resolução e antecipação de problemas relacionados a equipamentos de rede.

**PALAVRAS-CHAVE:** Gerenciamento de redes, Zabbix, SNMP, Resiliência em redes.

# ANALYSIS AND NETWORK MANAGEMENT USING A PROACTIVE METHODOLOGY WITH ZABBIX

## ABSTRACT

Before the growth of companies that adopt information technology as a strategic tool and control, network management arises as a need in an environment where the number of network devices increases as the time passes. Aimed at centralizing network management and low cost for implementation, this paper proposes the use of Zabbix tool and the SNMP protocol, not only for monitoring and control, but also for anticipation and resolution of problems related to network devices.

**KEYWORDS:** Network Management, Zabbix, SNMP, Resilience in networks.

HOLOS
ISSN 1807 - 1600

## 1 INTRODUÇÃO

O gerenciamento de equipamentos de tecnologia da informação vem se tornando comum diante da evolução de dispositivos que fazem uso de sistemas e serviços de rede. De acordo com o CETIC.br, no ano de 2013, 95% das empresas com até 49 funcionários já possuíam alguma tecnologia de rede, bem como rede sem fio, rede cabeada, intranet e extranet. Com isso, destaca-se que a TI vem sendo bem utilizada pelas organizações, e constitui para essas uma grande ferramenta estratégica no processo de planejamento, direção e controle. (PRATES; OSPINA, 2004).

Essa expansão, tanto de dispositivos como de equipamentos de rede, faz com que os serviços de tecnologia da informação que atuam nessas organizações e que dependem da rede para seu funcionamento, tenha um nível de disponibilidade maior, tornando evidente a necessidade de gerenciamento. Segundo Cestari Filho (2011)**,** o orçamento operacional, principalmente os custos com pessoal e os custos operacionais associados à manutenção dos sistemas de informação, representam a maior parte dos gastos, cerca de 70% de todo o gasto de TI em uma empresa típica. Os outros 30% são consumidos em desenvolvimento e aquisição de produtos. Portanto, o gerenciamento dos serviços de TI se tornam tão importante quanto a sua própria implantação.

De fato, o cotidiano das pessoas está relacionado diretamente com as redes de computadores, ofertando recursos que facilitam, por exemplo, a comunicação, e impactam, normalmente, em uma maior produtividade. Assim, manter o funcionamento de um serviço de TI, conforme esperado, sem um gerenciamento eficaz, é trabalhoso até mesmo em ambientes de pequeno porte. Além disso, existe a questão do gerenciamento centralizado, pois não é viável a equipe de TI utilizar diversas ferramentas diferentes para monitorar diversos equipamentos distintos, nesse caso ocorrendo um problema, talvez demore mais tempo para detectar essa falha do que simplesmente resolvê-la.

Neste contexto, o objetivo do presente artigo é mostrar o desempenho de uma ferramenta de monitoramento não somente de uma forma de analítica, e sim de uma forma proativa e centralizada, sem a intervenção do administrador para tratar de problemas considerados comuns. Ou seja, o sistema poderá ser capaz de detectar anomalias pré-determinadas no ambiente de rede e tomar ações no intuito de resolver, minimizar e até mesmo se antecipar a um problema, em um menor espaço de tempo. O trabalho consiste na combinação do uso da ferramenta Zabbix (normalmente usado de forma passiva no monitoramento de ativos, links, servidores, aplicações, etc.) e do protocolo SNMP *(Simple Network Manager Protocol*) no monitoramento de ativos para analisar estatisticamente parâmetros como tempo de disponibilidade, quantidade de tráfego dos links, de maneira a diminuir ou evitar a indisponibilidade do sistema em questão.

## 2 FUNDAMENTAÇÃO TEÓRICA

O protocolo SNMP basicamente consiste em um conjunto de operações simples e as informações contidas nessas operações, possibilitando ao administrador da rede ou aos serviços de TI (o qual necessita da rede para operar) a capacidade de coletar dados de dispositivos e até alterar o estado dessas informações, como por exemplo, mudar o estado de uma interface, verificar a velocidade em que a interface de um equipamento como *switch* ou roteador, saber a temperatura desses dispositivos, entre outros.

HOLOS ISSN 1807 - 1600

O protocolo SNMP é definido pela *IETF (The Internet Engineering Task Force)*, essa sendo responsável pelos padrões de protocolos que controla o tráfego de internet. O documento que especifica e indica normas para uso dos diversos protocolos é chamado de RFC *(Requests for Comments)*.

O SNMP conta com três versões, sendo definido inicialmente na RFC 1157, com base em palavras ou senhas, permitindo que qualquer aplicação baseada nesse protocolo pudesse se comunicar com outra aplicação através desse método de reconhecimento, palavras essas que são conhecidas como comunidades. O acesso a informação de gerenciamento de um dispositivo é realizado das seguintes formas: somente leitura, leitura e escrita e *trap.* Já na segunda versão do SNMP, as mudanças foram mínimas, ressalva a adição de mais dois comandos *getbulk* e *inform,* o primeiro facilita a recuperação de dados em tabelas, já o segundo possibilita a estratégia de gerenciamento descentralizado, isto é, uma comunicação entre gerentes e não somente gerente e agente. A terceira e mais recente versão foi desenvolvida com intuito de garantir segurança nos aspectos de autenticidade e criptografia em trocas de mensagens entre as entidades. “Apesar do SNMPv1 ser histórico, é ainda a principal implementação do SNMP que muitos fornecedores suportam”. (MAURO; SCHMIDT, 2005).

## 2.1 Entidades e Base de Informação de Gerenciamento

No ambiente do protocolo simples de gerenciamento (SNMP), existem duas entidades fundamentais: o gerente e o agente. O primeiro, que lida com a função de gerenciar a rede, comumente é um servidor, o qual através de um software realiza consultas de informações pela rede ao agente (switch, roteador, servidor Linux, servidor Windows, etc.) e esse responde.

A Figura 1 identifica uma consulta do gerente ao seu agente e esse último respondendo a solicitação, isso pode ser invertido quando utiliza-se o *trap*, ou seja, é uma maneira que o agente tem de avisar ao sistema gestor de rede que algo de errado ocorreu, enviando de forma assíncrona, sem necessidade de requisições por parte do gerente, entretanto, não será abordado esse método no trabalho.

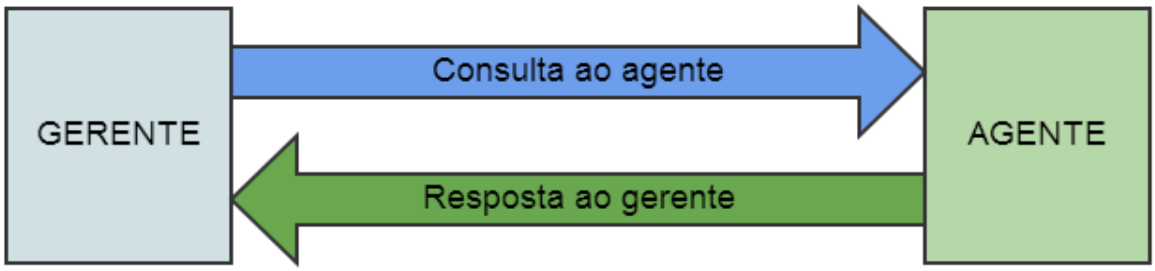


**Figura 1: Comunicação SNMP entre gerente e agente.**

As entidades possuem uma lista de objetos correspondentes as informações reais dos dispositivos e seus comportamentos, essas informações são armazenadas na MIB *(Management Information Base* - **Base de Informação de Gerenciamento***)*.

> A *Management Information Base* (MIB) pode ser pensada como um banco de dados de objetos gerenciados que o agente rastreia. Qualquer tipo de status ou informação estatística que pode ser acessado pelo gerente é definida em uma MIB. (MAURO; SCHMIDT, 2005)

HOLOS ISSN 1807 - 1600

A organização dos objetos é feita pelo SNMP, esse trata todas as MIB de uma forma hierárquica como em uma árvore, e são chamadas de OID *(object identifier)*, que são números inteiros separados por pontos baseados nos nós de toda árvore.

## 2.2 Modos de Operações do SNMP

A coleta de informações é realizada por meio de comandos do protocolo simples de gerenciamento de rede (SNMP), e cada comando tem seu formato de mensagem definidos para os gerentes e agentes utilizarem para receber e enviar as informações.

Toda operação SNMP utiliza por padrão o UDP (*User Datagram Protocol)* como protocolo de transporte das mensagens e a porta 161. Esses aspectos o torna pouco confiável, haja vista a falta de reconhecimento de pacotes perdidos, competindo a aplicação SNMP determinar se os datagramas estão perdidos e retransmiti-los.

As duas operações mais utilizadas nesse estudo de caso são o GET e o SET. O primeiro tem como finalidade a requisição iniciada pelo gerente passando por parâmetro o endereço daquele objeto solicitado, no caso a OID, logo em seguida o agente responde com o comando *get-response* o dado correspondente. A operação SET é utilizado para alterar o valor de um objeto, mas o objeto deve ser definido na MIB como permissão de escrita. Essa alteração deverá ser feita na configuração do equipamento. O protocolo SNMP possui outros comandos que não serão abordados nesse artigo por não fazer parte do escopo.

## 2.3 A Ferramenta Zabbix

O Zabbix é uma ferramenta de código aberto de monitoramento e controle para equipamentos de rede e seus serviços. Oferece em seu sistema de alarmes a possibilidade de enviar e-mail em um eventual problema, mensagens de texto, e com um pouco mais de conhecimento da ferramenta é possível o envio de comandos remotos facilitando a solução de problemas. A aplicação Zabbix é distribuída com a administração centralizada via navegador WEB e o armazenamento dos dados em um banco de dados relacional, suportando as três versões do protocolo SNMP, a ferramenta possui um agente compatível com diversos sistemas operacionais tais como: Linux, Solaris, HP-UX, Open BSD, OS X, NT4.0, Windows XP, Windows 7, entre outros.

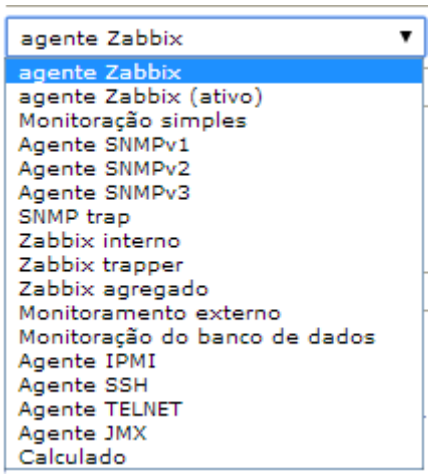


**Figura 2: Modos de coleta de dados por meio da ferramenta Zabbix.**

HOLOS ISSN 1807 - 1600

As coletas dos dados são feitas por meio de itens. Esses itens podem ser recolhidos através do agente Zabbix, do agente SNMP nas versões v1, v2 ou v3, por verificação simples de status como de um pacote ICMP *(Internet Control Message Protocol)* enviado a cada intervalo de tempo, por notificação pelo próprio cliente *(trapper)*, ou e até mesmo ser calculado. Este último se enquadra quando se faz junções de expressões dos itens, como por exemplo a média dos últimos dez valores armazenados. Existem outras formas de configurar essa coleta como mostra a Figura 2, então é uma questão de análise para a melhor escolha para o ambiente desejado.

Os alarmes do Zabbix são chamados de *triggers* ou gatilhos se traduzido para o português, definidos como uma expressão lógica que representa o status o item de monitoramento. O resultado dessa operação é recalculado sempre que o valor coletado por aquele item é alterado. A Figura 3 configura-se de um gatilho programado para que a ferramenta alerte quando uma determinada interface esteja desativada (*down*). A expressão é simplesmente o endereço (OID) onde a coleta vai ser realizada na MIB do cliente, com o nome do host e a forma que o valor será coletado e calculado (último valor, média, soma, intervalo de tempo). Apesar da configuração ter vários campos para serem configurados, o mais importante é a expressão e o campo risco, pois é nele que define-se o status de alerta conforme a importância desse alarme.

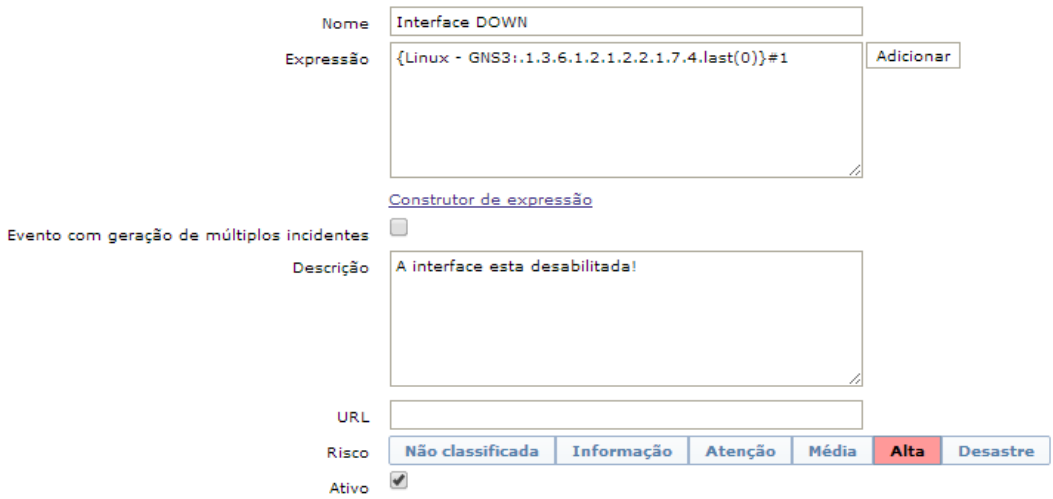


**Figura 3: Exemplo de configuração de *Trigger*.**

Diante de um alarme, ações podem ser tomadas, podendo ser um envio de e-mail, alerta visual ou sonoro e até mesmo comando remoto, ou seja, o Zabbix poderá perceber um evento pré-determinado e executar algum tipo de comando pré-configurado na tentativa de resolver o problema sem intervenção de nenhum administrador de TI. A Figura 4 exibe um exemplo de configuração de ação feita na ferramenta de monitoramento e controle. As operações da ação definem qual o tipo de ação a ser executada, nesse caso é executar um comando remoto, além disso, existe a lista alvo, isto é, o host ou grupo de host que irão receber essa ação. No exemplo citado, é feito a configuração de script personalizado no tipo de ação, o comando vai ser executado diretamente do servidor Zabbix até a máquina cliente. No campo Comandos, foi indicado o local de onde estará o *shell script* que enviará o comando SNMP SET até a interface do cliente. Por fim, existe o campo de condições, porém não será usado.

HOLOS
ISSN 1807 - 1600


**Figura 4: Exemplo de configuração de uma ação.**

Para uma maior flexibilidade, a ferramenta Zabbix suporta diversos comandos para coleta de informações pré-definidos, chamados de macros, que podem ser utilizados em situações como o de monitorar o status de um serviço específico, saber qual a quantidade de processamento que um servidor está utilizando. Essas macros têm uma sintaxe especial e o objetivo é economizar tempo e tornar a configuração do item mais transparente. O usuário também pode criar sua própria macro, fazer uso de combinações com as macros padrão do Zabbix e ainda adicionar operações matemáticas ou booleanas nessas operações. A Figura 5 exibe uma série de expressões que são disponibilizadas pela ferramenta Zabbix para serem usadas como macros.

| | |
|---|---|
| net.tcp.listen[port] | Checks if this port is in LISTEN state. 0 - it is not, 1 - it is in LISTEN state. |
| net.tcp.port[<ip>,port] | Check, if it is possible to make TCP connection to the port number. 0 - cannot connect, 1 - can con |
| net.tcp.service.perf[service,<ip>,<port>] | Check performance of service "service". 0 - service is down, sec - number of seconds spent on con |
| net.tcp.service[service,<ip>,<port>] | Check if service is available. 0 - service is down, 1 - service is running. If ip is missing 127.0.0.1 is |
| perf_counter[counter,<interval>] | Value of any performance counter, where "counter" parameter is the counter path and "interval" pa |
| proc.mem[<name>,<user>,<mode>,<cmdline>] | Memory used by process with name name running under user user. Memory used by processes. Pr |
| proc.num[<name>,<user>,<state>,<cmdline>] | Number of processes with name name running under user user having state state. Process name, |
| proc_info[<process>,<attribute>,<type>] | Different information about specific process(es) |
| service_state[service] | State of service. 0 - running, 1 - paused, 2 - start pending, 3 - pause pending, 4 - continue pendin |

**Figura 5: Lista de macros que podem ser utilizadas para monitoramento no Zabbix.**

## 3 METODOLOGIA

Para se fazer o teste do Zabbix aplicado a um ambiente virtual, foi realizado um teste de desempenho da ferramenta e do protocolo SNMP, como uma solução “proativa”. Com o auxílio da ferramenta de emulação GNS3 *(Graphical Network Simulator 3)*, foi montando um ambiente com um roteador Cisco modelo c7200 conforme a Figura 6:

HOLOS
ISSN 1807 - 1600

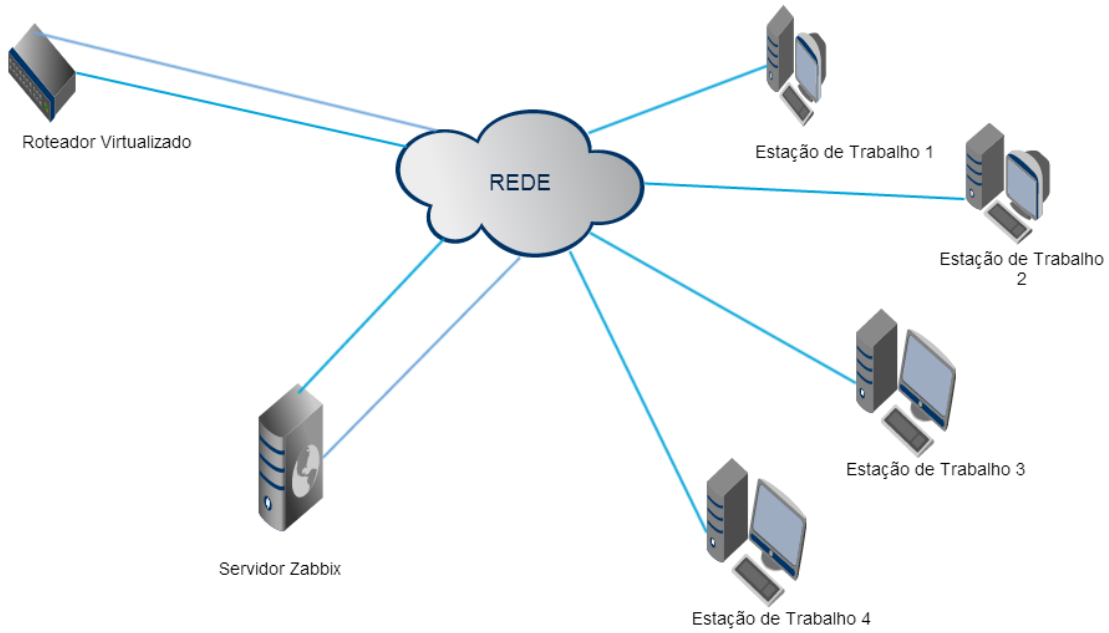


**Figura 6: Topologia elaborada para o estudo de caso.**

Na Figura 6, é visto também, que a conexão do servidor Zabbix monitora um roteador virtualizado no *software* GNS3, aquele atuando como ferramenta de monitoramento e de gerência proativa. Para realizar esse teste se fez necessário duas interfaces conectadas ao roteador, justamente para que seja realizado a conversão de uma rede para outra e o servidor Zabbix pudesse ter uma interface de diagnóstico.

Em seguida, foi testado o tempo em que uma das interfaces converge para a outra interface redundante, e para isso foi estabelecido alguns parâmetros de conexão e tamanho do pacote, nesse teste, foi empregado quatro conexões enviando pacotes ICMP *(Internet Control Message Protocol)* de tamanhos 32 *bytes*, 64 *bytes*, 256 *bytes* e maiores do que 1500 *bytes* com a intenção de explorar se o tamanho do pacote, tráfego ou até a fragmentação iria influenciar de alguma forma no tempo de restabelecimento do link. Vale salientar que os sistemas operacionais Linux e Windows enviam por padrão um pacote ICMP a cada segundo e embora esse tempo pode ser especificado ao executar o comando, foi utilizado como padrão de intervalo nesse trabalho.

Um segundo teste foi aplicado em um ambiente de rede real. Neste experimento, foi configurado dois switches, quatros máquinas clientes, além do servidor Zabbix. As estações de trabalho estão conectadas diretamente ao switch 1 e dois links interligam esse equipamento até o *switch* 2, sendo um deles desativado. Gerando um tráfego ICMP das máquinas clientes até o switch 2 e propositalmente desativando a porta do switch 2 conforme o 'X' na Figura 7, foi possível observar através do SNMP o Zabbix transferindo o tráfego para o segundo *link* em amarelo, que no primeiro momento estava desativado.

HOLOS
ISSN 1807 - 1600

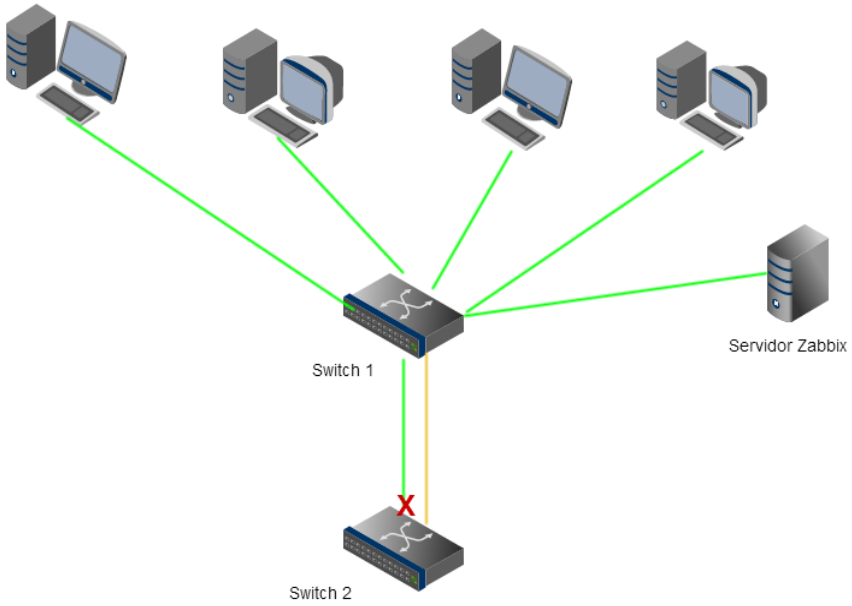


**Figura 7: Topologia utilizando um ambiente real.**

A ação do Zabbix no caso acima, é enviar comando SET SNMP, alterando o status da OID "*ifAdminStatus"* de "*down"* para "*up"* (e vice-versa), conforme permite a RFC 1213 responsável pela MIB II. O retorno desse comando pode ser o valor em inteiro 1 (um) em caso de *up*, 2 (dois) para a situação de *down*, e 3 (três) para ocasião de teste, sendo essa última pouco utilizada. A Figura 8 mostra o exemplo da ação da ferramenta Zabbix, diante de um possível problema apresentado em um roteador. A seta de cor verde indica um problema ao servidor Zabbix, esse servidor identifica o problema e gera uma ação por meio do *script* configurado na seção anterior, representado com a seta na cor verde.

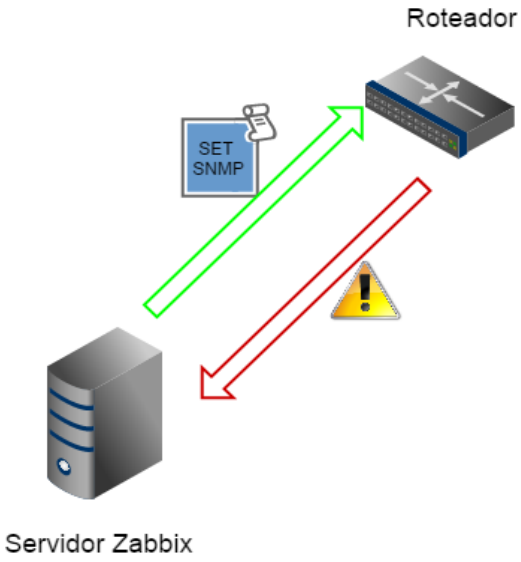


**Figura 8: Servidor Zabbix enviando um comando SNMP, diante de um problema identificado.**

HOLOS
ISSN 1807 - 1600

## 3.1 Analise de Tendência

A intenção da ferramenta de agir proativamente é justamente diminuir esforços do administrador na resolução de problemas, preparando o Zabbix para emitir alertas e tomar ações com base no histórico. Um tráfego considerado alto poderia representar diversos problemas na rede: aumentando congestionamento de pacotes, diminuindo o desempenho de determinados serviços e até mesmo parar a rede. A ferramenta Zabbix pode sim, ser configurada para esperar esse tipo de problema e gerar uma ação a partir disso, essa ação pode ser habilitar um novo servidor para balanceamento de carga ou tráfego, uma nova rota em um equipamento de camada rede, uma nova interface para escoamento desse tráfego. Entretanto, o tempo em que o Zabbix levaria para executar essa ação e de fato ficar em funcionamento, talvez durasse mais tempo do que simplesmente esperar a normalização de um pico em um curto intervalo de tempo. A ideia é fazer com que a ferramenta possa entender que a coleta daquele tráfego represente uma tendência, isto é, indicando que o tráfego vem exercendo um aumento conforme um intervalo de tempo configurável.

Desta forma, pretende-se construir uma tendência em relação a um período de tempo, isso faz com que seja possível analisar um comportamento padrão ou anômalo sob aquele período ou intervalo, tornado o sistema mais robusto.

Para tratar de tendência, foi aplicando a formula chamada de Móvel Média Exponencial (MME), essa, combinada com outras técnicas, são popularmente usadas para analises de mercado financeiro, de acordo com El-khodary (2009). A Equação 1 mostra a média móvel exponencial da forma que é usada pelos analistas financeiros**:**

**MME = (Preço atual - MME anterior) * K + MME anterior** Equação (1)

Onde:

$K = \frac{2}{N+1}$

A constante “K” é responsável por atribuir maior ou menor peso para o valor em vigor na tendência, dependendo se a diferença é negativa ou positiva. A constante “N” executa a quantidade de amostras.

A média móvel exponencial é conhecida por tratar melhor os valores analisados do que média simples, em testes preliminares foi percebido que a MME representa melhor o estado da rede em situações de picos, e faz sentido para a aplicação usada nesse artigo. Como já descrito anteriormente, possui variáveis que correspondem a tendências de mercado financeiro, com isso foi realizado uma adaptação para que a configuração juntamente com o Zabbix fosse possível analisar e até mesmo tomar decisões com base no que tráfego passado, ou seja, a tendência é representada pela média dos valores em um período de cinco minutos, subtraindo o último valor coletado, multiplica o fator “K” que soma a média dos valores no mesmo intervalo de cinco minutos. Lembrando que todos esses valores podem ser adaptados, a Equação 2 exibe a adequação:

$$\boldsymbol{Tendência} = \boldsymbol{Média}(\mathbf{300}\boldsymbol{s}) - \text{ú}\boldsymbol{ltimo\ valor} * \boldsymbol{K} + \boldsymbol{Média}\ (\mathbf{300}\boldsymbol{s}) \qquad \text{Equação (2)}$$

No Zabbix, a configuração foi realizada pelo agente Zabbix e um host Linux Debian 7.0, criando um item do tipo calculado, ficando da seguinte forma, consoante figura 9:

HOLOS
ISSN 1807 - 1600

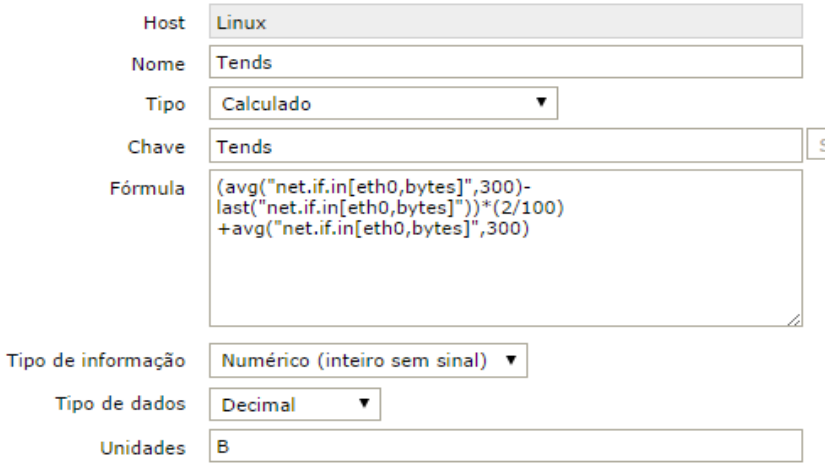


**Figura 9: Configuração de item calculado no Zabbix.**

Por uma questão didática e melhor entendimento, o histórico para a análise de tendência foi de cinco minutos e pelo mesmo motivo citado a constante 'K' foi de 0,02 – isto é, 2 (dois) dividido por 100 (cem). Ainda, foi utilizado a aplicação Iperf: uma ferramenta que afere teste de performance de uma interface, para que assim fosse gerado tráfego nessa interface e dessa forma avaliar o efeito da média móvel exponencial como tendência.

## 4 RESULTADOS EXPERIMENTAIS

Os resultados obtidos com o cenário descrito anteriormente foram satisfatórios em relação ao desempenho da ferramenta quanto a reabilitação da comunicação, alcançando o tempo mínimo de 12 (doze) segundos, independentemente do tamanho do pacote, conforme mostra a tabela 1:

**Tabela 1 - Tempo de convergência dos *links* em um ambiente virtualizado**

| Máquinas | 1 conexão | 2 conexões | 3 conexões | 4 conexões |
|---|---|---|---|---|
| 32 bytes | 16 | 19 | 17 | 19 |
| 64 bytes | 18 | 20 | 23 | 21 |
| 256 bytes | 22 | 21 | 20 | 18 |
| > 1500 bytes | 16 | 12 | 23 | 14 |

Tendo em vista que o ambiente foi virtualizado, alguns fatores de hardware como eficiência de processamento e memória que incorporam o ambiente de virtualização, podem ter influenciado a comunicação de rede, logo os resultados não trariam transparência.

No ambiente real, construído com *switches* foi analisado o mesmo experimento citado acima, ou seja, o tempo em segundos que a interface sofreu para reabilitar uma nova interface com tráfego passante, de acordo com a Tabela 2:

HOLOS ISSN 1807 - 1600

**Tabela 2 - Tempo de convergência dos *links* em um ambiente real**

| | 1 conexão | 2 conexões | 3 conexões | 4 conexões |
|---|---|---|---|---|
| 32 bytes | 8 | 10 | 9 | 18 |
| 64 bytes | 21 | 25 | 11 | 25 |
| 256 bytes | 29 | 35 | 32 | 8 |
| > 1500 bytes | 33 | 27 | 29 | 12 |

A variação do tempo de convergência é mínima em relação a conectividade de uma possível utilização de usuários na rede, comprovando de fato, que independentemente do tamanho do pacote (desses testados) não existe influência no tempo de convergência, assim como no ambiente virtualizado.

Já a análise de tendência avaliou o tráfego da rede baseado no histórico. Isso trouxe uma melhor resposta para o estado da rede em um determinado intervalo de tempo. Com isso, é possível realizar uma ação apoiado na linha de base do gráfico de análise de tendência, conforme a Figura 10:

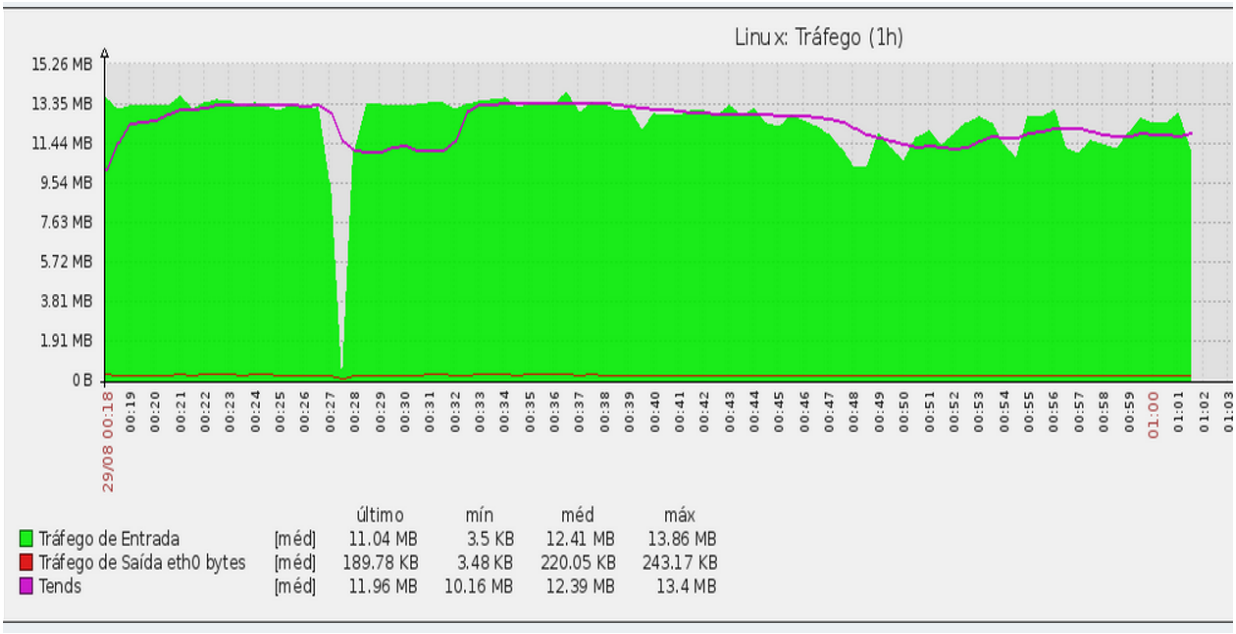


**Figura 10: Análise de tendência com gráfico de tráfego de rede.**

O trecho preenchido em verde representa o tráfego real da rede, já a linha na cor roxo identifica o estado ou tendência do tráfego real, adaptando a formula de média móvel exponencial ao estudo desse caso. Nessa figura 10, fica claro perceber no instante de tempo por volta 00:26 que o tráfego da rede chega a quase 0 bytes por segundo, todavia, a linha de base identifica essa queda do link e passa a se comportar em baixa, a partir do instante 00:28 o tráfego tem um pico de 0 bytes a 13.35 megabytes e a linha de tendência continua a desempenhar um comportamento previsível fundamentado nos últimos cinco minutos.

## 5 CONSIDERAÇÕES FINAIS

Apesar de saber das deficiências do protocolo SNMP nas versões 1 e 2 no quesito segurança, o experimento trouxe resultados positivos em relação a importância do gerenciamento de redes, independente do cenário, seja virtual ou real.

Ainda é legítimo afirmar que a ferramenta Zabbix também pode ser utilizada para tomadas de decisões em um inesperado incidente de indisponibilidade de um equipamento de rede como roteador ou *switch*, além disso, comprova que mesmo em uma situação com tráfego alto, não existe influência significativa na reabilitação de uma interface.

Com o auxílio da ferramenta Iperf, foi possível gerar tráfego em máquina de sistema operacional Linux, e assim adaptar uma equação de análise de tendência de mercado para a realidade de gerência de redes, obtendo uma tendência na rede ao qual permite a ferramenta que agora toma decisões, passe a resolver problemas antes mesmo que essa anomalia ocorra. Isso sem intervenção direta de um administrador de redes, ou seja, agindo de forma proativa.

Pode-se concluir que o gerenciamento centralizado é essencial para redes de computadores, e o auxílio da ferramenta Zabbix torna mais fácil controlar e gerenciar a redes, como também resolver e antecipar a problemas rotineiros.

Por fim, é possível em trabalhos futuros, testar a performance das experiências realizadas nesse artigo com o protocolo SNMP na versão 3, onde a princípio, os problemas de segurança que a versão 1 (um) e 2 (dois) tem, foram sanados com essa última versão, possibilitando autenticação e criptografia.

## 6 REFERÊNCIAS

1. CESTARI FILHO, Felício. Gerenciamento de Serviços de TI. Rio de Janeiro: RNP/ESR, 2011. 242p.
2. CETIC BR. A5 - PROPORÇÃO DE EMPRESAS COM REDE (LAN, INTRANET E EXTRANET). 2013. Disponível em: <http://www.cetic.br/tics/empresas/2013/geral/A5/>. Acesso em: 10 jun. 2014.
3. EL-KHODARY, I. A. A decision support system for technical analysis of financial markets based on the moving average crossover. World Applied Sciences Journal, 6(11):1457–1472, Cairo, 2009.
4. GNS3 (Org.). Introduction to GNS3. Disponível em: <http://www.gns3.net/>. Acesso em: 06 jun. 2014.
5. ILLINOIS, The Board Of Trustees Of The University Of (Org.). The TCP/UDP Bandwidth Measurement Tool. Disponível em: <https://iperf.fr/>. Acesso em: 08 jun. 2014.
6. INTERNET ENGINEERING TASK FORCE. RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB II. California: Performance Systems International Editors, 1991.
7. MAURO, Douglas R.; SCHMIDT, Kevin J.. Essential SNMP. 2. ed. California: O'reilly Media, 2005.
8. PRATES, Glaúcia Aparecida; OSPINA, Marco Túlio. Tecnologia da informação em pequenas empresas: fatores de êxito, restrições e benefícios. Revista de Administração Contemporânea, Curitiba, v. 8, n. 2, p.09-26, jun. 2014.

HOLOS
ISSN 1807 - 1600

9. WAWRZENIAK, Diego. Média Móvel Exponencial: Como e Quando Utilizar? Disponível em: <http://blog.bussoladoinvestidor.com.br/media-movel-exponencial/>. Acesso em: 01 ago. 2014.
10. ZABBIX SIA (Org.). Introdução ao Zabbix. Disponível em: <https://www.zabbix.com/documentation/pt/1.8/manual/sobre/introducao_ao_zabbix>. Acesso em: 31 jul. 2014.
11. ZABBIX SIA (Org.). Zabbix Documentarion: Configuration. Disponível em: <https://www.zabbix.com/documentation/1.8/manual/config>. Acesso em: 23 jun. 2014.