Redes de Computadores II

Aula 15 - Gerenciamento de Redes – Parte III

Apresentação

Em aulas passadas, estudamos protocolos e ferramentas que nos permitem administrar e gerenciar uma rede de computadores. Todo esse conhecimento é necessário, pois uma rede, após projetada, instalada e configurada, exige ser mantida para continuar a operar adequadamente. Essa manutenção é realizada mais facilmente a partir de um monitoramento contínuo de todos os elementos presentes na rede, desde os equipamentos físicos até os protocolos e serviços em execução.

Nesta aula, aprenderemos a trabalhar com uma ferramenta que ganha cada vez mais espaço em pequenas, médias e grandes corporações: o software **Zabbix**.

Objetivos

Ao final desta aula você será capaz de:

- Entender o que é Zabbix;
- Compreender o funcionamento da arquitetura de monitoramento de redes do Zabbix;
- Conceituar definições utilizadas no Zabbix e em outros softwares de monitoramento.

Introdução

Um monitor de rede é um sistema que indica o desempenho (lentidão ou não funcionamento) de dispositivos de rede. Esse monitoramento é baseado na análise do *throughput*, taxas de erros, perda de pacotes, latência, tempo de resposta e disponibilidade dos roteadores e dos switches. Se alguma falha ocorre, o administrador da rede deve receber uma notificação sobre a falha, por meio de um alerta em sua estação de trabalho, um e-mail, um telefonema ou outros modos de contato.

O monitoramento de rede também possibilita a otimização do fluxo de dados e a detecção de equipamentos não confiáveis. Além disso, pode verificar a capacidade dos dispositivos e as suas condições operacionais, tais como temperatura e taxa de utilização. Como resultado, o monitoramento de rede ajuda a maximizar o desempenho da rede e a minimizar o potencial de falhas e erros.

Comumente, o monitoramento de rede é confundido com técnicas que oferecem condições relativas à segurança, como a prevenção de a rede ser acessada por usuários não autorizados. Para esse tipo de segurança, existem os IPS (*Intrusion Prevention Systems*) e IDS (*Intrusion Detection Systems*), ferramentas a serem estudadas na disciplina de Segurança de Redes. Monitoramento de rede é utilizado somente para análise da utilização da rede e para monitoramento relativo à confiabilidade da rede. O monitoramento de rede é suportado por uma vasta categoria de equipamentos, tais como servidores, roteadores e *switches*, podendo, ainda, ser empregado em diversos tipos de redes, como LANs, WLANs, VPNs e até WANs.

Atividade 01

1. Faça uma pesquisa e defina a diferença entre monitoramento de rede baseado em agente (*agent-based*) e monitoramento sem agentes (*agentless*).

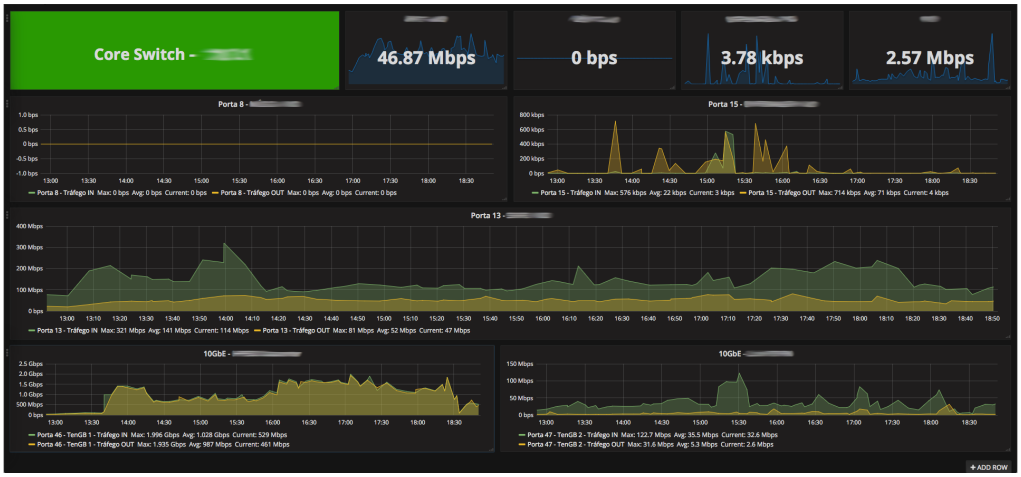
Zabbix

O Zabbix é uma ferramenta de monitoramento de redes, a qual atua como um monitor centralizado da disponibilidade e do desempenho da rede e dos dispositivos desta. Se uma falha ocorre, um alerta notificará o administrador da rede por telefone ou por e-mail. O *software* Zabbix é totalmente gratuito, distribuído segundo a licença GPLv2.

O Zabbix não tem limitações em relação à quantidade de equipamentos monitorados e, oficialmente, permite que a comunidade faça alterações em seu código-fonte. Além disso, o Zabbix suporta qualquer dimensão de rede: desde redes pequenas até grandes redes corporativas. O time responsável por manter o Zabbix disponibiliza periodicamente atualizações e novas versões.

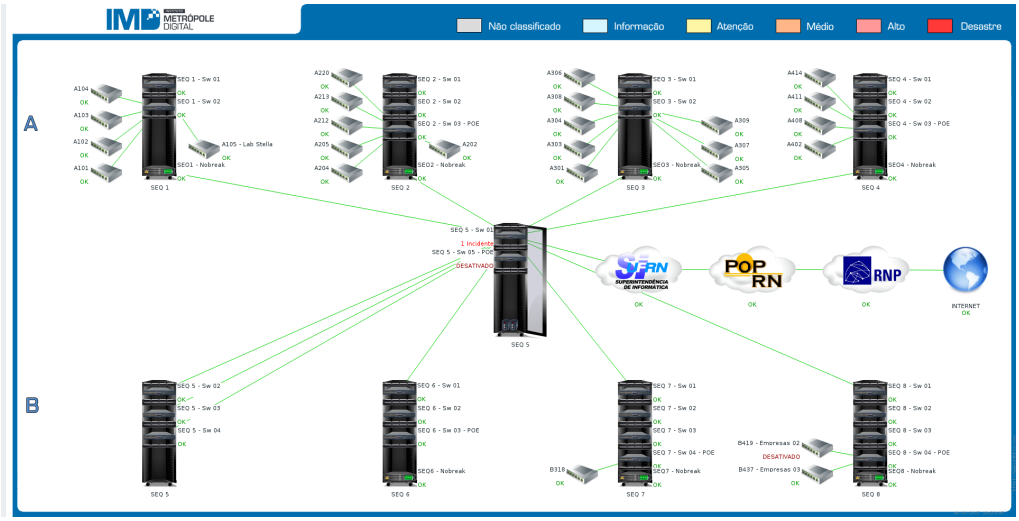
Para você ter uma ideia de quão poderosa é essa ferramenta, exemplos de empresas e instituições que utilizam o Zabbix no Brasil são: a Caixa, a CAERN, a UFRN, a USP, o TJ-RN e a Petrobras. Nas Figuras 1 e 2, você pode ter a noção de como é a interface de monitoramento da rede e dos equipamentos através do Zabbix.

Figura 01 - Exemplo de tela de monitoramento do Zabbix.



Fonte: DTI-IMD-UFRN.

Figura 02 - Exemplo de um mapa da rede monitorado pelo Zabbix.



Fonte: DTI-IMD-UFRN.

História e Funcionalidades do Zabbix

O *software* Zabbix foi desenvolvido em 1998 por Alexei Vladishev, o qual, naquele tempo, atuava como administrador de sistemas em um banco. Ele era o responsável por manter e gerenciar os bancos de dados e, a fim de automatizar algumas tarefas rotineiras, desenvolveu o primeiro protótipo do Zabbix.

Na época, havia poucas opções de gerenciadores de rede no mercado: HP Open View e IBM BMC, ambas soluções proprietárias, caras e complexas para serem configuradas e mantidas.

Após 3 anos, em 2001, a primeira versão do Zabbix (1.0 *alpha*) foi disponibilizada para a comunidade. Em 2017, o Zabbix se encontra na sua versão 3.4 (a logomarca do *software* pode ser vista na **Figura 3**).

Figura 03 - Logomarca do *software* de monitoramento Zabbix.

Fonte: http://www.zabbix.com

O Zabbix oferece diversas funcionalidades para seus usuários. Uma delas é o suporte ao monitoramento de dispositivos de rede, como roteadores, *switches* e servidores, tanto para o monitoramento baseado em agente (com a instalação de *software* localmente nos dispositivos) quanto sem a utilização de agentes. Para o monitoramento, os dispositivos devem suportar o protocolo SNMP, estudado anteriormente, e, então, o Zabbix permite monitorar a disponibilidade e o desempenho deles.

Outra interessante funcionalidade do Zabbix é a possibilidade do gerenciamento e do monitoramento de máquinas virtuais. Essa poderosa ferramenta de monitoramento também permite a verificação em tempo real de bancos de dados e de *web services*.

Definições

O Zabbix define algumas convenções em relação a nomenclaturas:

Temos o ***host***, o qual diz respeito a todo ativo de rede, servidor ou qualquer outro dispositivo que possua um IP. Como exemplos de *hosts*, podemos citar roteadores, *switches*, servidores *web*, impressoras, pontos de acesso, etc.

Todo *host* precisa pertencer a um **grupo**, o qual normalmente agrupa *hosts* de um determinado tipo ou função, objetivando facilitar a administração. Exemplo: grupo ‘servidores’, grupo ‘switches’, grupo ‘desktops’, grupo ‘impressoras’, grupo ‘Natal’, etc.

O Zabbix define também o conceito de **item**, o qual trata de qualquer ponto a ser monitorado dentro de um *host*. Por exemplo, um item pode ser um disco, uma memória ou uma resposta a *ping*. Itens também podem ser serviços, como o HTTP, o NTP, o DNS, entre outros.

Os ***templates*** são agrupadores de itens, servindo como uma base comum para a utilização em servidores ou ativos de rede semelhantes. Dessa forma, evita-se o retrabalho de configurar manualmente *host* a *host*. Por exemplo, um *template*

chamado ‘Template OS Linux’ contém diversas configurações específicas para o monitoramento de um dispositivo que possua o Linux como sistema operacional. Um *host* pode ter diversos *templates* associados.

Os ***triggers*** monitoram itens em relação a valores. Por exemplo, se a utilização de uma CPU ultrapassar 80%, se o espaço em uma determinada partição estiver menor que 5Gb, ou se um determinado *switch* não responder a um *ping*. Em casos assim, um *trigger* disparado pode, então, realizar algum tipo de ação, como enviar um e-mail para o administrador da rede.

Os **eventos** são gerados após a ativação de um *trigger*, e dizem respeito a registros que permitem uma análise histórica das atividades e ações realizadas durante o monitoramento.

E, por fim, as ***actions*** são ações realizadas em decorrência da ativação de um *trigger*,. Como exemplos delas, temos o envio de mensagens, a execução de comandos remotos, etc.

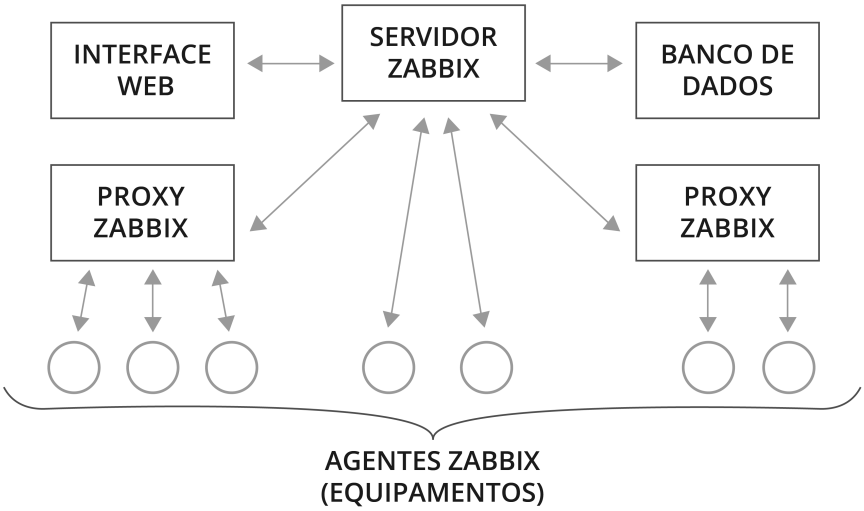
Atividade 02

1. Com base em seu conhecimento acerca de redes de computadores, cite dois exemplos de *triggers* que podem ser úteis na administração de uma rede.
2. Busque, na documentação do *software* Zabbix, dois exemplos de operações de *actions* que podem ser configuradas após um *trigger* ter sido ativado.

Arquitetura do Zabbix

A arquitetura do Zabbix consiste nos seguintes componentes: o servidor Zabbix, o *proxy* Zabbix, o agente Zabbix e a interface *web*. Cada componente tem o seu papel pré-definido no monitoramento. A Figura 4 ilustra a arquitetura completa que contém todos esses componentes.

Figura 04 - Arquitetura do Zabbix.



Fonte: autoria própria

O **servidor Zabbix** é o núcleo do Zabbix. Sua principal função é desempenhar o monitoramento remoto da própria rede e dos seus componentes. O servidor também armazena configurações, histórico e dados operacionais. Se um erro ocorrer, o servidor Zabbix entrará em contato com o administrador da rede.

O ***proxy* Zabbix** coleta dados a fim de serem posteriormente transmitidos ao servidor Zabbix. A utilização de *proxies* é opcional, porém é uma solução bastante benéfica para distribuir a carga computacional de um único servidor Zabbix.

O **agente Zabbix** desempenha o monitoramento local de dispositivos de rede. Ele monitora recursos como discos rígidos, memória e estatísticas da utilização de CPU. Para monitorar esses recursos, é necessário que o agente esteja localmente instalado em cada equipamento.

A **interface *web*** é a camada de interação entre o Zabbix e o administrador da rede. Essa camada faz parte do servidor Zabbix e, normalmente (mas nem sempre), é executada na mesma máquina na qual o servidor está em execução.

Em suma, a combinação dos diferentes componentes do Zabbix permite três diferentes tipos de monitoramento: verificação simples, agente Zabbix e verificação externa. A verificação simples monitora a disponibilidade de diversos serviços, como SMTP e HTTP, sem instalações adicionais no servidor remoto. O agente Zabbix são

aqueles que monitoram localmente a utilização do hardware. Por fim, a verificação externa desempenha o papel de monitoramento através do SNMP, do IPMI (*Intelligent Platform Management Interface*), do SSH e do Telnet.

Note que na arquitetura ilustrada também pode ser visto um outro componente: o banco de dados. O banco de dados Zabbix é responsável por armazenar dados históricos.

É interessante ressaltar que o monitoramento com o Zabbix pode ser realizado sem a utilização de *proxies*. Nesse caso, todos os dados de monitoramento são coletados diretamente pelo servidor Zabbix.

Atividade 03

1. Qual a importância da utilização de um banco de dados em um sistema de monitoramento como o Zabbix?
2. Utilizando seu conhecimento em redes de computadores, indique um simples utilitário/ferramenta que não é baseado em agentes e pode ser utilizado como forma de monitoramento da disponibilidade de um servidor?

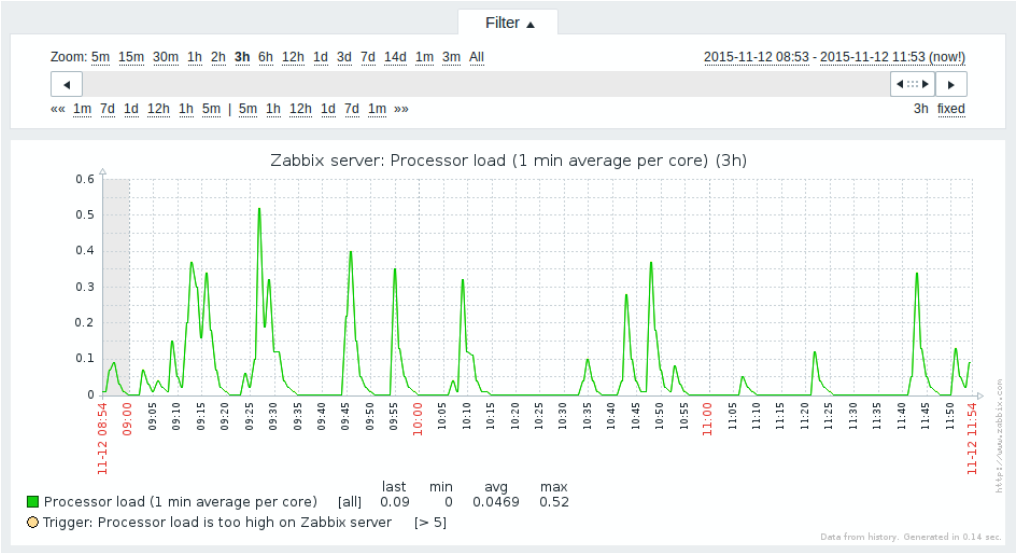
Vantagens do Zabbix

O *software* Zabbix é uma ferramenta robusta e confiável, no que diz respeito ao monitoramento de redes. Se o Zabbix alerta o usuário sobre alguma falha, esse usuário pode ter plena confiança da existência do problema. Além disso, uma das grandes vantagens da utilização do Zabbix é o fato de ele ser escalável, de modo a podermos empregá-lo em redes de pequeno, médio e grande porte, moldando-se à realidade da rede em questão.

O Zabbix também conta com um sistema de alertas altamente configurável e personalizável. Notificações podem ser configuradas para envio de acordo com *triggers*, com destinatários, com o tipo de notificação (e-mail SMS, etc.), e é possível, ainda, definir ações que automaticamente executarão comandos remotos.

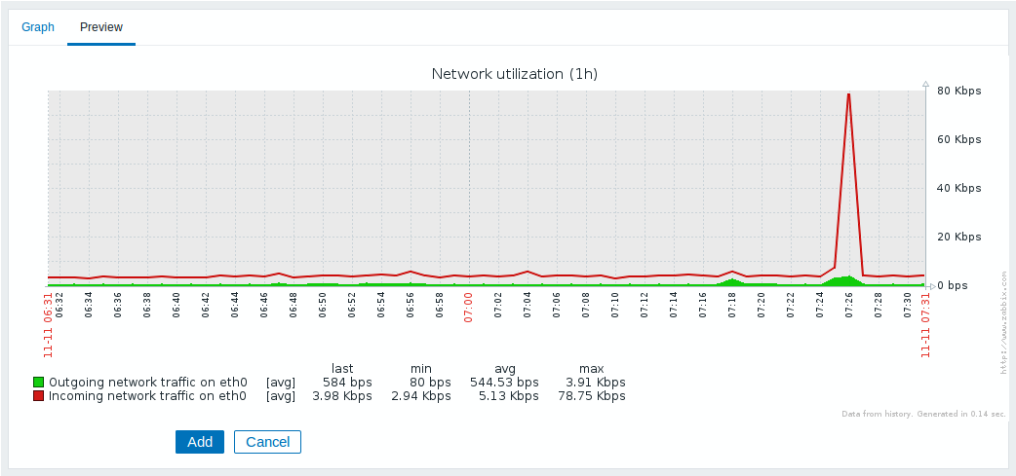
Outro aspecto bastante atrativo da utilização do *software* de monitoramento Zabbix é a geração de gráficos em tempo real, na qual itens monitorados são imediatamente atualizados por meio de gráficos. Esses gráficos podem ser gerados automaticamente simplesmente após a adição de um item. Na Figura 5, é mostrado um exemplo da utilização da CPU de um equipamento, apresentando-nos os gráficos simples. Os gráficos compostos, por sua vez, permitem o cruzamento de diferentes dados, como o tráfego de entrada e de saída em uma determinada interface de um equipamento de rede, conforme ilustrado na **Figura 6**.

Figura 05 - Exemplo de gráfico simples.



Fonte: Documentação do Zabbix 3.4

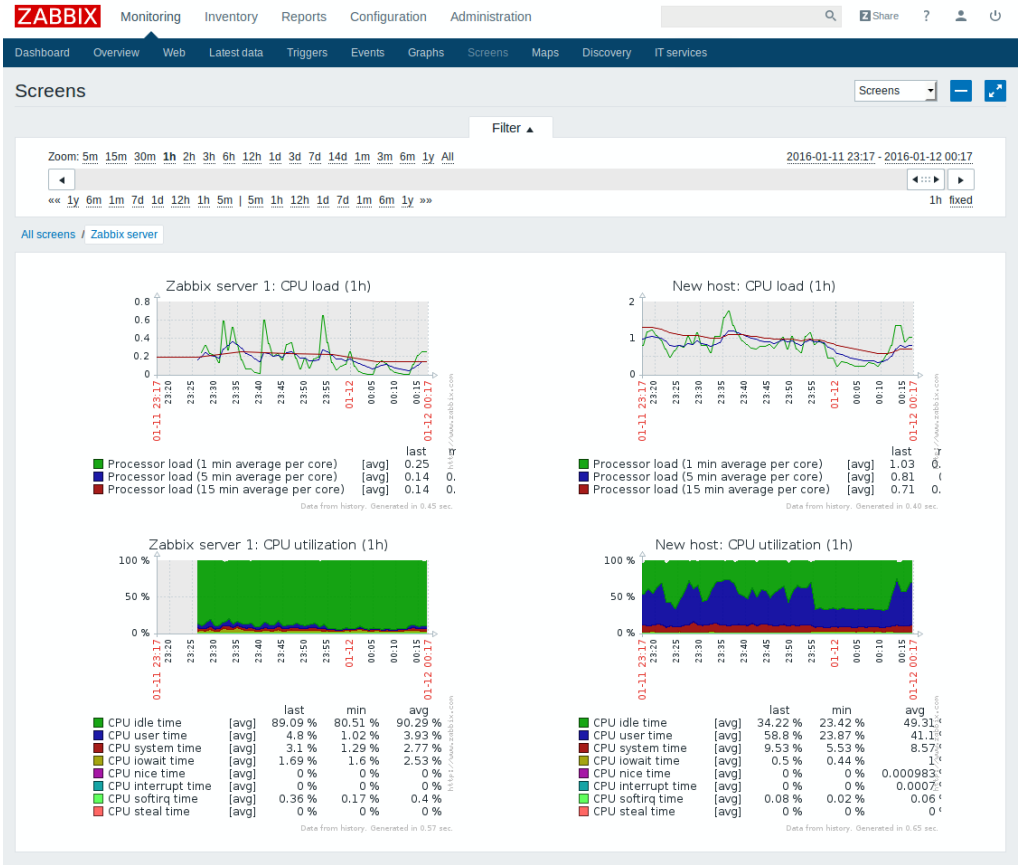
Figura 06 - Exemplo de gráfico composto.



Fonte: Documentação do Zabbix 3.4

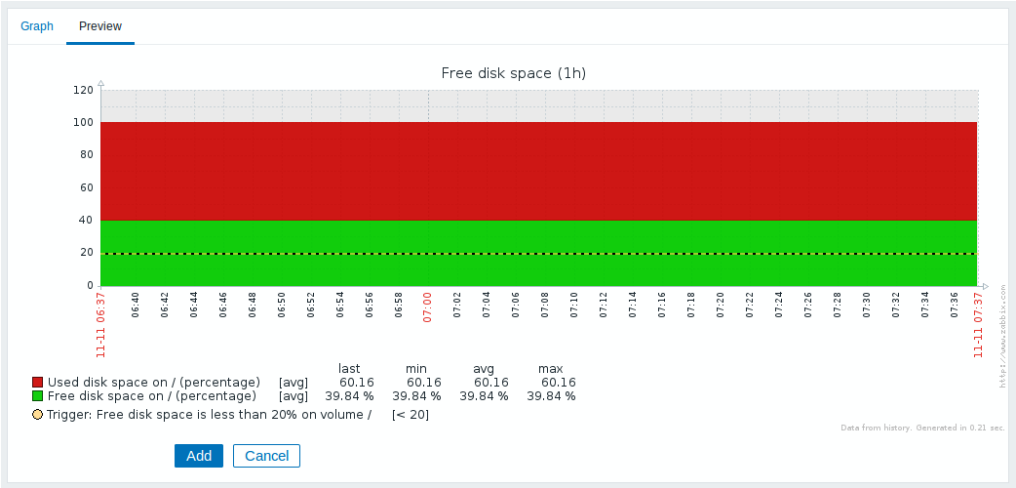
A utilização de gráficos é bastante customizável, permitindo a criação de telas que apresentam diversas complexidades e informações, conforme a tela da Figura 7. Outro exemplo interessante é o gráfico relativo à utilização de espaço em um disco, tratando tanto do espaço livre quanto do espaço utilizado. Sobre esse exemplo, é ilustrada, na Figura 8, a linha que delimita um *trigger* (indicada em 20%).

Figura 07 - Gráficos são utilizados para monitoramento visual de itens.



Fonte: Documentação do Zabbix 3.4

Figura 08 - Gráfico composto com indicação de um *trigger*.



Fonte: Documentação do Zabbix 3.4

O armazenamento de dados históricos também é uma característica do Zabbix. Por meio da utilização de banco de dados, é possível guardar dados históricos, permitindo, assim, por exemplo, o estudo de um caso específico que ocorreu no passado.

Por fim, outra vantagem do Zabbix é a API (*Application Programming Interface*) disponibilizada pelo *software*, possibilitando que outros desenvolvedores integrem facilmente seus programas com o Zabbix, para adquirirem os dados obtidos por ele.

Atividade 04

---

1. Qual a diferença entre gráficos simples e gráficos compostos?
2. Pesquise na Internet e cite alternativas gratuitas e *open-source* para o *software* de monitoramento Zabbix.

Resumo

Nesta aula, estudamos uma excelente ferramenta para otimizar o processo de gerenciamento e monitoramento de redes de computadores: o Zabbix. Além de ser gratuito e *open-source*, o Zabbix traz diversas funcionalidades essenciais para todo administrador de redes e sistemas. Por meio de intuitivas interfaces gráficas, é muito mais fácil realizar a análise da saúde da disponibilidade dos ativos de rede e os serviços executados sobre ela.

Autoavaliação

1. Durante as aulas desta disciplina, você conheceu diferentes exemplos de *softwares* para monitoramento e gerenciamento de redes. Destaque as principais vantagens das ferramentas CACTI e Zabbix, realizando uma comparação entre estas.

Referências

Andrea Dalle Vacche, Stefano Kewan Lee. *Zabbix Network Monitoring Essentials*. Packt Publisher 2015.

Adail Horst, Aécio Pires, André Luis. *De A a Zabbix*. Editora Novatec. 2015.

Documentação oficial Zabbix 3.4. Disponível em https://www.zabbix.com/documentation/3.4/start.