ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB

Ferramenta de monitoramento de redes Zabbix

Rodrigo Eduardo Araújo Silva

Resumo

Monitorar redes não é somente colocar todos os ativos em funcionamento e esperar que os mesmos parem de responder ou funcionar, mas verificar a eficácia e o funcionamento dos equipamentos na infraestrutura sendo ela empresarial ou residencial garantindo um funcionamento contínuo e um elevado grau de qualidade no serviços. É importante entender que o aumento da utilização de redes de computadores fez que aumentasse também o número de problemas que ocorrem na mesma, fazendo com que o monitoramento de uma rede seja necessário para garantir sua eficácia. Este estudo teve o objetivo de analisar a ferramenta de monitoramento de redes Zabbix e sua praticidade que faz com que seja tão utilizada na atualidade e assim conhecer sua arquitetura capaz de auxiliar administradores de redes na prevenção de vulnerabilidades. Este estudo teve o objetivo de analisar Zabbix, uma ferramenta de monitoramento de ativos de rede e sua praticidade, uma ferramenta livre que dispõe da criatividade do administrador para monitorar qualquer ativo da rede, sendo ela local ou externa. Dentre os autores pesquisados para a constituição conceitual deste trabalho, destacaram-se Andrew Stuart Tanenbaum (2003), Jim Kurose (2009), Janssen Dos Reis Lima (2014), Werneck Bezerra Costa(2013) e André Luis Boni Déo (2012). A metodologia utilizada foi a pesquisa explicativa, tendo como coleta de dados o levantamento bibliográfico. As conclusões mais relevantes foram que o Zabbix se mostrou uma ótima opção para monitoramento de rede, pois não há nenhum investimento financeiro para utiliza-la. Possui uma interface de fácil compreensão e uma excelente apresentação de resultados de forma visual através de gráficos e relatórios.

Palavras-chave: Zabbix, Monitoramento, Redes.

1 Introdução

Com o grande crescimento tecnológico de redes corporativas e o uso intensivo da informação nos negócios, um serviço ou um ativo que a mesma possua ficando minutos fora do ar, pode acarretar grande perda financeira para algumas empresa por isso o presente estudo delimita-se a estudar e compreender o funcionamento básico da ferramenta livre de monitoramento de redes Zabbix para fins de monitoramento de servidores e serviços;

O presente estudo delimita-se a estudar a ferramenta de monitoramento de redes Zabbix, uma ferramenta livre que possui o intuito de monitoramento de ativos de rede para ajudar na gestão de equipamentos para prevenção de falhas e grandes desastres através do protocolo de rede snmp.

Diante dessas situações de falha o monitoramento em tempo real de ativos, serviços ou até mesmo de infraestruturas completas é completamente indispensável, quanto mais rápido e preciso for a identificação do problema antes mesmo que ele aconteça em uma infraestrutura ou ativo mais rápido e fácil será a tomada de decisão para resolução de problemas com isso o objetivo geral é compreender e analisar o funcionamento da ferramenta de monitoramento de redes livre Zabbix;

Esta pesquisa justifica-se a aprender o funcionamento básico para monitoramento de ativos e serviços de rede, assim evitando o downtime prolongado e prevenção de desastres entre equipamentos e serviços críticos para empresas e instituições para que não sejam prejudicadas por falhas de hardware (discos rígidos com pouco espaço, placas de rede defeituosas e serviços parados que necessitam ser levantados manualmente);

A metodologia deste trabalho é a pesquisa explicativa, tendo como coleta de dados o levantamento bibliográfico, apurando e observando todos os dados pertinentes a este estudo.

2 Rede de Computadores

Pode-se definir como rede de computadores um conjunto de dispositivos conectados por uma única tecnologia para uso comercial, compartilhando recursos a todos os usuários com políticas estabelecidas e para uso pessoal para acesso de conteúdos remotos, entretenimento e comunicação (TANENBAUM, 2003).

Atualmente é impossível imaginar uma empresa que não utiliza uma rede de computadores para troca de informações. O trafego de dados em uma rede corporativa faz aumentar a preocupação com a segurança das informações compartilhadas. De acordo com Tanenbaum (2003) a segurança em redes de computadores é a preocupação em garantir que pessoas mal-intencionadas não consigam ler ou alterar qualquer informação enviada a outro destinatário.

Para prover a segurança em uma rede de computadores é necessário entender como uma rede é gerenciada. Para isso é necessário conhecer o conceito de gerencia de redes e as principais áreas de gerenciamento.

3 Gerenciamento de Redes

No início do uso das redes de computadores, os problemas que surgiam eram facilmente identificados com simples procedimentos. Devido seu avanço e a grande utilização da internet, onde temos vários aparelhos ligados com milhões de pessoas conectadas, torna-se necessário a utilização de ferramentas especificas para a identificação e solução dos problemas de uma rede para que a mesma continue efetiva. Desta forma surgiu o gerenciamento de redes que foi dividido em cinco principais áreas: gerenciamento de desempenho, gerenciamento de falhas, gerenciamento de configuração, gerenciamento de contabilização e gerenciamento de segurança (ABREUS; PIRES, 2009; KUROSE; ROSS, 2009).

O gerenciamento de desempenho define se uma determinada rede está com um bom desempenho. Este gerenciamento tem o objetivo de quantificar, medir, informar, controlar e analisar o desempenhos dos componentes ligados a uma rede. O protocolo SNMP (*Simple Network Management Protocol*) tem papel fundamental para gerenciar o desempenho na internet.

O gerenciamento de falhas tem como meta identificar, encontrar e corrigir problemas físicos ou lógicos em uma rede. Há sistemas de gerenciamento que trabalham na antecipação de falhas para garantir que a rede esteja sempre em funcionamento.

O gerenciamento de configuração está relacionado ao inventario de uma rede que permite um administrador saber quais os componentes fazem parte de uma determinada infraestrutura além da sua configuração e seus registros.

O gerenciamento de contabilização gerencia os registros, logs ou bilhetes para contabilizar a utilização dos recursos da rede permitindo que o administrador de rede registre e controle o acesso de usuários e dispositivos aos recursos da rede.

O gerenciamento de segurança: tem como meta regularizar e gerenciar o acesso aos recursos de redes e de determinadas informações através de políticas bem estruturadas. Sendo assim inclui tarefas como verificar os privilegio de acesso dos usuários e detectar e registrar tentativas de acesso não autorizados.

Para monitorar uma rede estruturada existem três etapas. A primeira etapa consiste na coleta de dados, relatórios, gráficos e tabelas sobre cada usuário armazenado em arquivos de log. A segunda etapa consiste no diagnóstico obtido através dos dados coletados e a identificação da causa dos problemas ou falhas detectadas. A terceira etapa consiste na ação ou controle sobre o recurso (DEO, 2012).

Sendo assim, um conjunto de softwares de um sistema de gerenciamento é estruturada para assumir o papel de gerente, agente ou de ambos. Como gerente permite a aquisição e o envio das informações de gerenciamento por meio de comunicação com um ou mais agentes. Como agente, utiliza software especifico presente nos dispositivos gerenciados que tem o objetivo de atender as requisições enviadas pelo gerente. O modelo de gerenciamento SNMP também conhecido como modelo de Internet apresenta componentes como gerente e agente como citado anteriormente (DEO, 2012).

Para melhor entendimento, na seção a seguir é apresentado os conceitos ligados ao protocolo SNMP.

4 Protocolo de Gerenciamento

O protocolo utilizado no gerenciamento de redes é o SNMP (Simple Network Management Protocol), que é um protocolo da camada de aplicação que permite colher informações sobre o estado dos dispositivos das redes. Suas interações são sem conexão utilizando o protocolo UDP/IP para troca de mensagens através das portas 161 e 162 com pacotes de tamanhos variáveis (DÉO, 2012; FERREIRA, 2008).

O SNMP possui dois componentes: o Agente SNMP e Gerente SNMP. O Agente SNMP é um software instalado em qualquer dispositivo da rede com a função de manter contadores que informam o estado do equipamento, como trafego de pacotes nas interfaces de um roteador. O Gerente SNMP é um software com a função de solicitar as informações aos agentes SNMP para interpretação e apresentação para o administrador de rede e também possibilita a configuração remota via SNMP (FERREIRA, 2008).

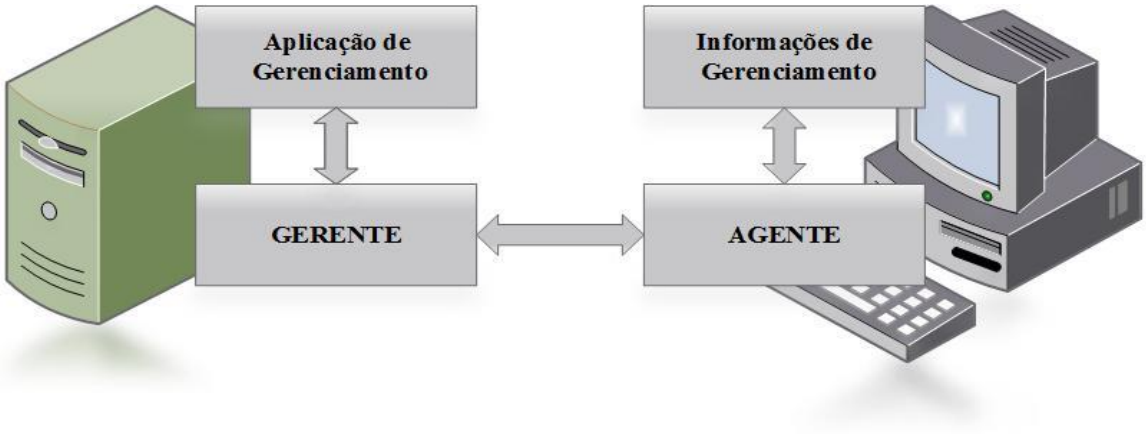

Figura 1: Monitoramento via SNMP
Fonte: Deo (2012)

As informações de gerenciamento são armazenadas em MIBs (Management Information Base) que é um arquivo com a função de atribuir um nome, um número e um conjunto de permissões a cada contador. Este arquivo também fornece uma descrição do que os contadores representam (DÉO, 2012; FERREIRA, 2008).

As MIBs são definidas através de SMI (Structure of Management Information) que é a linguagem usada para definir as informações de gerenciamento que fazem parte de uma entidade gerenciada de rede para certificar que a sintaxe e a semântica dos dados de gerenciamento de rede sejam bem definidas e sem ambiguidades (DÉO,2012; KUROSE; ROSS, 2009).

A versão mais recente do SNMP é a SNMPv3 que foi lançada em abrril de 1999 e atualizada em dezembro de 2002 e substituiu as versões SNMPv1 e SNMPv2 (KUROSE; ROSS, 2009).

5 Software de gerenciamento Zabbix

Segundo Lima (2014) sobre o Zabbix:

> Zabbix foi criado por Alexei Vladishev em 1998. A ideia surgiu quando trabalhava em um banco na Letônia como administrador de sistemas, pois não estava satisfeito com os sistemas de monitoramento que estava trabalhando na época. (LIMA, p. 7, 2014).

O Zabbix controla a disponibilidade e desempenho de aplicações, ativos e serviços de rede, que faz uso de SGBD (Sistema de Gerenciamento de Banco de Dados) para manter configurações e dados armazenados (HORST; PIRES; DÉO, 2015). Possui a capacidade de monitorar com apenas um servidor milhares de itens. É possível também ter um monitoramento distribuído permitindo um servidor central de monitoramento e vários outros servidores secundários enviando as métricas para o servidor principal ou apenas replicando informações, sendo possível separa também outros servidores como o servidor web, servidor de banco de dados e servidor de monitoramento para aumentar sua performance (LIMA, 2014).

O Zabbix possui diversos módulos onde os mais utilizados são Servidor Zabbix, Banco de dados, Interface web, Agente Zabbix, Proxy Zabbix e Java Gateway. O Servidor Zabbix é o elemento central com verificação remota dos serviços e é a ligação entre os agentes e o proxy Zabbix. Ele manipula as informações em relatórios com alertas para execução de ações pré configuradas. O Banco de dados é acessado via interface web e via servidor Zabbix para

configuração e informações. A interface web é o ambiente para configuração do Zabbix. O Agente Zabbix é uma aplicação cliente que envia dados sobre os equipamentos ao servidor monitorando o estado de aplicativos, serviços e hardware. O Proxy Zabbix recebe os dados de funcionamento e status em benefício do servidor Zabbix. O Java Gateway é uma versão do Zabbix com suporte para aplicações Java com o objetivo de restaurar os contadores do JMX (Java Management Extensions) (HORST; PIRES; DÉO, 2015).

A arquitetura Zabbix está organizada em três camadas: aplicação, banco de dados e a interface web. A camada de aplicação é demonstrada pelo back-end que faz a coleta dos dados nos ativos de rede. A camada de banco de dados é demonstrada pela base de dados responsável pelo armazenamento das informações coletadas pelo back-end e passar para o front-end. A camada interface web é demonstrada pelo front-end que dá acesso a informações de monitoramento aos administradores e fornece informações para aplicações que utilizam o Zabbix (LIMA,2014).

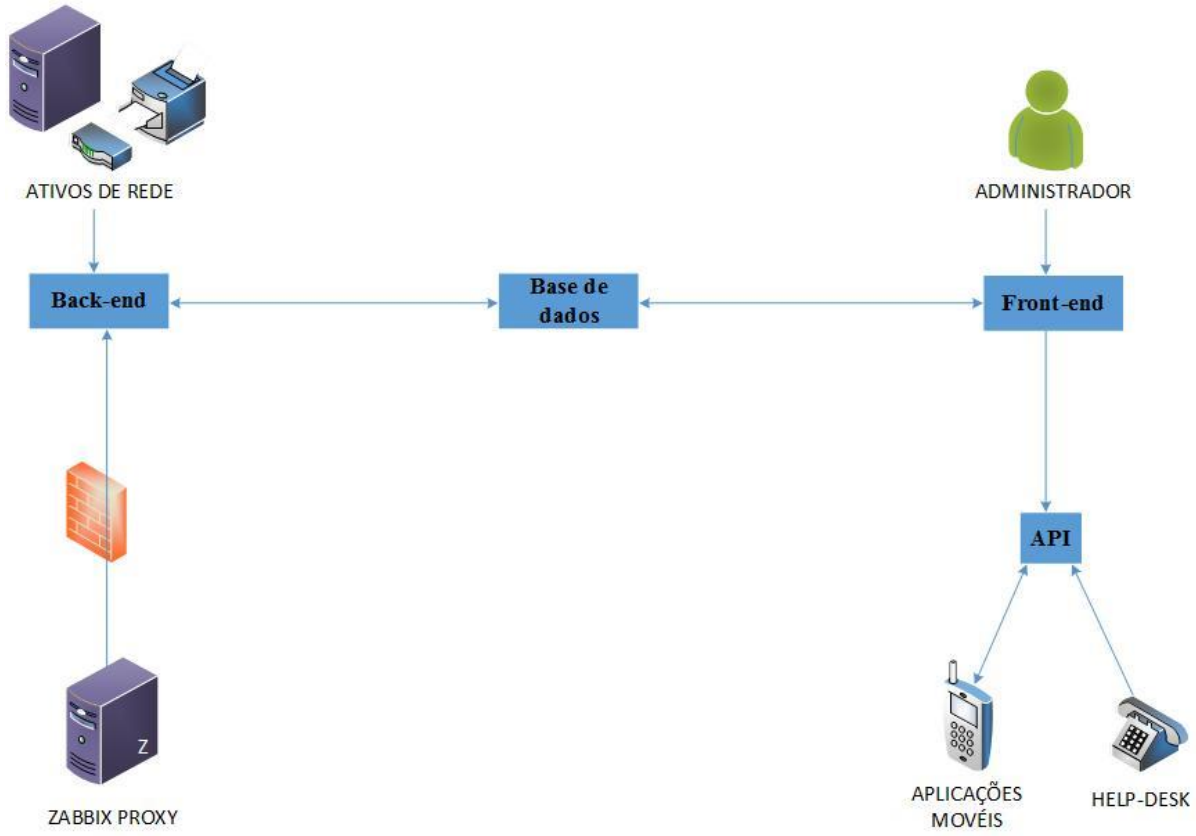

Figura 2: Arquitetura Zabbix
Fonte: Lima (2014)

Na arquitetura do Zabbix há três elementos que fazem parte do back-end que é responsável pelas principais funções: Zabbix Server, Zabbix Proxy e Zabbix Agent (LIMA, 2014).

O Zabbix Server é o sistema em que os agentes remetem ao back-end que armazena os dados coletados.

O Zabbix Proxy é um elemento opcional já que o Zabbix server não depende dele para funcionar. É um host responsável por colher dados de clientes remotos para transmitir ao Zabbix Server;

O Zabbix Agent é o cliente que reporta para o Zabbix Server.

Os requisitos mínimos para a instalação do Zabbix são 128 MB de RAM e 256 MB de espaço livre em disco rígido com um processador Pentium II no mínimo. Como a aplicação utilizará banco de dados que serão atualizados automaticamente é necessário maior espaço em disco e memória física. Se a área a ser monitorada for muito extensa com grande número de dispositivos é aconselhado o uso de um servidor apenas para o banco de dados separadamente do Zabbix Server para que assim não haja uma concorrência de recursos como processador e memória (LIMA, 2014).

Para o seu funcionamento, também é necessário a instalação de alguns softwares: Apache; PHP com suporte BC, XML, session, socket, multibyte; PHP GD; MySQL; Oracle; IBM DB2; PostgreSQL; SQLite (LIMA, 2014).

É necessário também a instalação de dependências para a compilação do código fonte. As dependências necessárias são: Compilador C; Automake; MySQL.

Ao utilizar o Zabbix é importante lembrar que o mesmo possui várias opções de monitoramento, que em um ambiente de produção é necessário após a instalação, a configuração das opções que serão utilizadas. É possível também a escolha do SGBD que deseja utilizar, não sendo necessário a instalação dos demais SGBD's listados anteriormente.

Uma característica do Zabbix é que ele suporta vários SGBD's como o MySQL/Mariadb, SQLite, Oracle, PostgreSQL e IBM DB2. Os módulos responsáveis pelo sincronismo e coleta de dados foram desenvolvidos em linguagem C e a sua interface web em PHP. Ele possui diversas funcionalidades: detecta os dispositivos de rede automaticamente; detecta o recurso do host de forma automática por simples verificação, utilizando o sistema agente ou por SNMP; LLD que possibilita a criação automática de triggers, itens e gráficos para diversos objetos descobertos no host monitorado; Administração controlada através de proxy via web com monitoramento distribuído; Sistema servidor compatível com os sistemas operacionais Mac OS X, OpenBSD, NetBSD, FreeBSD, GNU/Linux, IBM AIX, Solaris, HP-

UX, AIX e GNU/Linux; Sistema agente compatíveis com os sistemas operacionais Mac OS X, OpenBSD, NetBSD, FreeBSD, GNU/Linux, IBM AIX, Solaris, HP-UX, AIX e GNU/Linux Windows; Monitoramento independente da utilização do sistema agente; Auditoria do sistema; Alertas via e-mail, SMS, Jabber XMPP e scripts personalizados; Monitoramento de aplicações web, aplicações Java, ambientes virtualizados e dispositivos via IPMI (Intelligent Platform Management Interface) (HORST; PIRES; DÉO, 2015).

A comunicação entre o Agente e o Zabbix Server pode ser realizada de cinco formas diferentes que pode variar de acordo com o tipo do item a ser coletado do dispositivo gerenciado (HORST; PIRES; DÉO, 2015).

Uma forma é através do Protocolo TCP, porta 10050 (Zabbix Agent Passivo) onde Zabbix Server se conecta ao dispositivo gerenciado e solicita os itens que o usuário configurou para coleta e o agente Zabbix sempre aguarda a solicitação do Zabbix Server.

A segunda forma é pelo Protocolo TCP, porta 10051 (Zabbix Agent Ativo) onde o dispositivo gerenciado se conecta ao Zabbix Server, recebe a lista dos itens a serem monitorados, coleta os dados conforme o passado pelo Zabbix Server e o envia periodicamente.

A terceira forma é pelo Protocolo TCP, porta 10052 (JMX) que é um monitoramento usado em servidores de aplicação Java por meio do componente Java Gateway.

A quarta forma é pelo Protocolo UDP, porta 161 (SNMP) onde os dados coletados pelo Zabbix Server são aqueles que os fabricantes de equipamento implementaram conforme as normas RFC’s.

A quinta e ultima forma é pelo Protocolo UDP, porta 623 (IPMI) que é destinado ao monitoramento de recurso de hardware, ou seja, não depende do sistema operacional ter sido iniciado.

O Zabbix possui como formas de visualização de dados elementos como gráficos e mapas de rede entre outros que podem ser classificados como simples e composto. Os elementos simples são os gráficos simples, gráficos customizados e mapas de Rede. Os elementos compostos seria uma visão simultânea como por exemplo mapas de rede e gráficos, este recurso é denominado Screens (COSTA, 2015).

Por ser um software livre e devido os inúmeros módulos presentes para auxiliar no monitoramento, mostrando-se uma ferramenta completa, o Zabbix torna-se uma boa proposta para quem pretende monitorar e identifica riscos na rede.

6 Implementação de um gerenciamento de rede com Zabbix

A implementação de um gerenciamento utilizando o sistema Zabbix trouxe ao administrador de rede maior controle devido aos diversos módulos de gerenciamento proporcionando uma antecipação dos riscos de uma rede para que assim a manutenção seja preventiva ao invés de corretiva, além de auxiliar na tomada de decisão.

A instalação desta ferramenta é feita através de terminal onde deve ser seguido vários critérios. É instalado inicialmente o Zabbix Server para então instalar o Zabbix Agent de acordo com o sistema operacional e configurar os parâmetros para que os dados sejam enviados para o Servidor.

O Zabbix Server é um aplicativo rápido e estável que apresenta os resultados do monitoramento em tempo real em formato de gráficos e relatórios para melhor interpretação dos administradores de rede. Os arquivos de log gerados pelo Zabbix podem ser acessados pela interface gráfica ou pelo terminal (SANTOS, 2015).

7 Conclusão

O estudo apresentado teve como objetivo analisar a ferramenta de monitoramento de redes Zabbix e sua praticidade, abordando conceitos ligados ao monitoramento de redes. As vulnerabilidades em redes de computadores pode trazer sérios riscos aos negócios quando não monitoradas. A ferramenta Zabbix se mostrou uma ótima opção para monitoramento de rede. Além de ser uma ferramenta livre onde não é necessário nenhum investimento para utiliza-la, sua interface é de fácil compreensão e com uma apresentação de resultados visual através de gráficos e relatórios que auxilia o administrador de rede na tomada de decisão sem perda de tempo com a leitura de extensos relatórios.

Os alertas enviados por e-mail e por SMS, o acesso a logs e a verificação de memória e disco são altamente relevantes nas tomadas de decisão. Outro fato do banco de dados das vulnerabilidades atualizarem automaticamente. Estas características mostram que o Zabbix é uma ferramenta satisfatória e flexível. Desta forma pode-se concluir que Zabbix é uma ferramenta que atende perfeitamente um administrador de rede no objetivo de monitorar uma rede em tempo real com praticidade.

Referencias

ABREU, F. R.; PIRES, H. D. **Gerência de Redes**. Niterói - RJ, 2009.

COSTA, W. B. Monitoramento de rede: visão externa com abordagem de nuvem e software livre Zabbix. Natal, 2015.

DEO, A. L. B. **Gerenciamento de redes com SNMP**. Campinas: Agência para Formação Profissional da Unicamp, 2012. 151 f. Apostila.

FERREIRA, R. E. **Linux**: guia do administrador do sistema. 2. ed. São Paulo: Novatec Editora, 2008,

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

KUROSE, J. F.; ROSS, K.W. **Redes de Computadores e a Internet**: uma abordagem TopDown. Tradução Opportunitty Translations; Revisão técnica Waggner Zucchi. 5. ed. São Paulo, 2009.

LIMA, J. R. **Monitoramento de redes com Zabbix**. Rio de Janeiro: Brasport Editora, 2014

SANTOS, S. S. N. **Monitoramento de rede:** análise e configuração do software Zabbix. São Paulo, 2015

TANENBAUM, A. S. **Redes de Computadores**. 4. Ed. Campus, 2003