SEGURANÇA INFORMÁTICA E DAS COMUNICAÇÕES

- Ficha de Apoio -

CAPÍTULO 3. SEGURANÇA EM REDES E SISTEMAS (Monitoria)

1. Gestao de Redes

De acordo com Monteiro e Boavida (2011), consideram que as actividades de gestão de redes podem ser entendidas a vários níveis distintos, abrangendo aspectos que vão desde a monitorização de simples elementos de rede, até a gestão de redes complexas ou a gestão de serviços ou aplicações de processamento distribuído. Como exemplo de algumas actividades de gestão podem citar-se, entre outras, a avaliação de desempenho de um sistema, a detecção, isolamento e/ou correção de falhas, a contabilização e taxação, o controlo da configuração de equipamentos de rede, e a coordenação e controlo de mecanismos de segurança.

As necessidades de gestão fazem-se sentir quer no fornecedor dos serviços de comunicação, quer no utilizador desses serviços.

Os mesmos autores, defendem que à medida que aumenta a complexidade e dimensão de serviços suportados pelo fornecedor de serviços, as suas necessidades de resposta em termos de controlo, coordenação e monitorização aumentam, de modo a possibilitar a oferta dos serviços com a qualidade requerida. Idealmente, essas necessidades requerem uma forma de gestão integrada, que permita o acesso à informação de rede a diversos níveis.

Também o utilizador dos serviços de comunicação tem a necessidade de informação respeitante directa ou indirectamente ao funcionamento da rede, que lhe permita, por exemplo, negociar níveis de qualidade de serviço, tomar opções de funcionamento ou ainda, ser informado com a possibilidade de escolha de níveis de detalhe dos custos das comunicações efectuadas.

Estes aspectos tornam evidente a necessidade de incorporar de algum modo, no sistemas de comunicação, ferramentas para recolher, transferir, arquivar, analisar e apresentar informação de gestão de rede e para monitorar, controlar e coordenar os recursos de comunicação.

2. Função de Gestão

De acordo com Monteiro e Boavida (2011), os primeiros sistemas de gestão de redes centraram a sua funcionalidade na detecção e recuperação de falhas, dado que este era um dos aspectos mais importantes do ponto de vista da operação e de utilização das redes de comunicação. Com a evolução destas redes, as exigências em termos de qualidade de serviço requerida pelos e fornecida aos utilizadores alargaram-se a outra áreas funcionais, para além das falhas.

Tipicamente os diversos modelos e paradigmas de gestão assentam numa classificação de funções de gestão em cinco categorias, designadas por áreas funcionais de gestão, que são elas:

- Gestão de falhas;
- Gestão de configuração;
- Gestão de contabilização;
- Gestão de desempenho; e
- Gestão de segurança.

Gestão de falhas

Monteiro e Boavida (2011), consideram que consideram que a gestão de falhas é uma das áreas mais importantes na gestão de redes. Uma das actividades fundamentais na gestão de falhas consiste na detecção de erros. Após a detecção, terão que ser levadas a cabo acções de diagnóstico e recuperação

de erros.

A detecção de erros é feita com base em acções de monitorização de eventos, como seja a ocorrência de alarmes gerados por dispositivos de rede, a degradação do desempenho de rede ou componentes, ou a falha de aplicações.

O diagnóstico de erros é feito com base na análise dos erros detectados, uma falha conduzirá a vários alarmes e/ou erros correlacionados, cabendo as funções de diagnóstico a filtragem de erros correlacionados e a determinação da sua causa comum.

A detecção ou o diagnóstico de um erro podem conduzir à geração de uma notificação de problema, que levará a tomada de acções para a sua resolução, por parte do sistema ou de um operador/gestor.

Após a fase de detecção e diagnóstico de erros, é necessário desencadear acções de recuperação. Erros simples poderão requerer uma alteração de configuração de um elemento de rede ou sua substituição. Erros mais complexos poderão levar a reconfiguração de partes de redes ou intervenções de equipas de campo.

Gestão de configuração

Conforme expõe Monteiro e Boavida (2011), a gestão de configuração congrega um conjunto de funções para recolher, monitorar e alterar informação de configuração do sistema de comunicação, de forma a gerir alterações de hardware e/ou software.

A informação recolhida poderá ser usada, por exemplo, para a construção de visões topográficas da rede, abrangendo dispositivos de rede, ligações quer físicas assim como lógicas.

Gestão de contabilização

Segundo Monteiro e Boavida (2011), em redes cuja a utilização seja taxada, isto é, em redes comerciais, a gestão de contabilização assume um papel de primordial importância. As funções de contabilização são responsáveis pelo registo da utilização de recursos/serviços de rede por parte de utilizadores ou grupos, com o objectivo de se proceder a respectiva taxação.

Mesmo em redes comerciais, a contabilização da utilização de recursos pode ser uma actividade importante. Através dela, poder-se-á determinar padrões de utilização de recursos por parte dos utilizadores, o que poderá servir para determinação da qualidade no uso de recursos ou para a tomada de decisões sobre políticas de imposição de quotas de utilização. Apesar de nas redes não comerciais os utilizadores não serem taxados individualmente, os equipamentos e meios de comunicação tem custos de

aquisição e manutenção, sendo importante, em alguns casos, ter uma ideia sobre utilizadores ou grupos que mais recursos consomem, de forma a que seja possível reflectir sobre eles os custos de expansão e/ou actualização da rede.

A gestão de contabilização assume, ainda, um papel fundamental no suporte a auditorias, por exemplo para a determinação da utilização concreta de recursos por parte de um dado utilizador, o que é essencial para dar resposta a quesitos legais na área da prevenção da criminalidade informática.

Gestão de desempenho

Monteiro e Boavida (2011), afirmam que a gestão de desempenho congrega funções para a recolha e tratamento de dados relativamente ao comportamento dos objectos geridos, sendo essencial para o suporte de actividades de configuração, gestão de falhas e planeamento de rede.

Na sua forma mais simples, a gestão do desempenho pode reduzir-se a uma mera monitorização do estado dos elementos físicos ou lógicos da rede, para o registo numa base de dados de informação de gestão. Sistemas mais elaborados poderão utilizar a informação de desempenho para modelizar o comportamento da rede, diagnosticar problemas de rede, prever o desempenho futuro ou apoiar decisões de planeamento.

Gestão de segurança

De acordo com Monteiro e Boavida (2011), a segurança em ambiente de rede é, hoje em dia, uma preocupação indispensável, dada a globalização dos sistemas de comunicação. As funções de gestão de segurança preocupam-se com a monitorização e controlo dos mecanismos de segurança em utilização no sistema.

Algumas das actividade de gestão de segurança são a definição de utilizadores, grupos e respectivos privilégios, a identificação dos requisitos de segurança associados aos diversos recursos de rede, a configuração e monitorização de sistemas de segurança e o registo em *log* de ocorrências relevantes.

3. Plataforma para Gestão de Redes

Para Monteiro e Boavida (2011), a gestão dos actuais sistemas e redes informáticos exige a utilização de equipamentos e/ou plataformas de gestão especializados.

Se por um lado a utilização de equipamentos isolados de diagnóstico e teste como tentadores de cablagem

ou analisadores de protocolos possa ser importante para algumas actividades de monitorização e, até gestão de falhas, tal utilização não pode suprir as complexas necessidades da gestão de redes de média e grande dimensão, nas suas diversas áreas funcionais. Por outro lado algumas ferramentas mais elaboradas tais como certos analisadores de redes, têm funcionalidade acrescida, no entanto é frequentemente acompanhado por especificidade relativamente a fabricantes e/ou por ausência de interfaces para o desenvolvimento e expansão, o que as transforma em ferramentas fechadas.

As plataformas de gestão vêm responder as essas necessidades, fornecendo funcionalidades de gestão a diversos níveis, integrando os diversos ambientes protocolares de gestão e permitindo a gestão em todas as suas vertentes de redes heterogêneas de grande dimensão.

Características das plataformas de gestão de redes

Monteiro e Boavida (2011), são da opinião que em geral, as plataformas de gestão têm características que as tornam abrangentes, por um lado, e flexível, por outro. Dessas características salientam-se:

- Suporte de uma variedade de protocolos e tecnologias de gestão, quer abertos quer proprietários, tendo em vista conferir a maior abertura e abrangência possíveis;
- Possibilidade de integração com um leque alargado de recursos, independente de fabricantes e do seu tipo;
- Estrutura modular e distribuída, sendo possível a interação entre módulos localizados em sistemas diferentes;
- Utilização de modelos de dados evoluídos como, por exemplo, modelos baseados no paradigma *object-orented* e capacidades de interligação/interação com bases de dados relacionais;
- Interfaces normalizadas para interacção de gestão com outros sistemas;
- Interfaces para desenvolvimento, permitindo a interação de aplicações com diversos módulos da plataforma;
- Suporte a interfaces gráficas, através das quais é possível uma completa definição e controlo das actividades de gestão, de uma forma mais simples; e

Critérios de selecção de plataformas de gestão

Boavida *et all* (2012), afirmam que a selecção de uma plataforma de gestão carece da observação de

alguns critérios, uma vez que este tipo de equipamento implica um investimento considerável e é determinante para o controlo que os administradores da rede terão sobre a generalidade dos recursos de comunicação. Pelo menos os critérios abaixo deverão ser levados em consideração para a selecção da plataforma de gestão:

- **Funcionalidade**

O que um gestor de redes procura, em primeiro lugar, é a funcionalidade de gestão. É com as funções de gestão presentes na plataforma que ele terá que desempenhar grande parte das suas funções.

- **Extensibilidade**

A extensibilidade da plataforma é um critério que pode assumir particular importância em redes sujeitas a forte crescimento e/ou alterações frequentes. Trata-se de uma característica que, estando presente, confere uma grande capacidade de adaptação da plataforma a desenvolvimentos futuros, o que salvaguarda o investimento inicial.

A extensibilidade deve ser suportada por uma arquitetura modular escalável, que possibilite a adição de novos módulos funcionais, a interação entre módulos situados em sistemas diferentes e a delegação de actividades de gestão em módulos/subsistemas remotos constituindo subdomínios. Para além disso, é ainda desejável um elevado grau de portabilidade, de forma que a plataforma de gestão não fique restringida a um dado sistema de rede.

- **Abertura**

Cada vez mais os diversos sistemas de redes disponibilizam interfaces normalizadas para a gestão. Assim, o suporte de tecnologias normalizadas é essencial para a abertura da plataforma, que poderá interagir, deste modo, com equipamentos de diferentes fabricantes e diferentes natureza. A normalização constitui ainda, uma garantia de interoperabilidade com o equipamento a instalar futuramente.

Para além da normalização, é ainda importante que as plataformas de gestão suportem as mais correntes tecnologias e protocolos proprietários, dado que é frequente que as redes de comunicação comportem apenas equipamentos que possam ser geridos com essas tecnologias/protocolos.

- **Segurança**

Pela sua natureza, as operações de gestão são operações críticas em torno da

segurança. Através de operações indevidas de configuração, é possível tornar inoperável toda a rede de comunicação. É, assim, essencial que a plataforma de gestão seja dotada de mecanismos de segurança com especial ênfase na autenticação de operadores e no registo de histórico de operações que impeçam que utilizadores não autorizados utilizem a plataforma e que registem todas as operações efetuadas. Para além disso, devem existir ainda mecanismos de aviso, que alertem o operador para o risco de certas acções de gestão, sempre que estas estão prestes a ser executadas.

- **Actualização da tecnologia**

A plataforma deverá ser tecnologicamente actualizada, em termos de *hardware*, *software* de sistema operativo e *software* aplicacional. Deverão ser suportadas as tecnologias mais recentes, quer em termos de modelos de informação quer em termos de comunicação. É ainda, conveniente o suporte de interfaces *web*.

- **Aplicações**

Para além da funcionalidade básica de gestão normalmente associada às tradicionais áreas de gestão de redes, a inclusão de aplicações compostas de elevado nível de abstração, com possibilidade de automatização de um grande número de tarefas de gestão, é bastante desejável. É relativamente frequente que as aplicações suportadas comportem algum nível de inteligência, o que, em alguns casos, permite identificar problemas automaticamente e iniciar/propor acções correctivas, com um nível mínimo de intervenção do operador.

- **Custo**

Como em qualquer problema de engenharia, o custo é um factor determinante. Os diversos critérios anteriormente mencionados deverão ser adequadamente ponderados pelo custo da plataforma.

O custo de investimento inicial, compra da plataforma de gestão, é no entanto, apenas um dos factores de custo. A este factor a que juntar custos de manutenção e actualização da própria plataforma e, sobretudo, o custo dos recursos humanos para

a sua operação.

4. Tipos de Plataforma de Gestão

Plataformas comerciais

Segundo Boavida et all (2012), existe uma grande variedade de plataformas comerciais para a gestão de redes, desenvolvidas pelos principais fabricantes de equipamentos de software, ou empresas que trabalham em colaboração com eles. A seguir são apresentadas algumas características de plataformas de gestão consideradas representativas: *HP Software & Solutions* e *System Center Configuration Manager*.

HP *Software* & *Solutions*

Esta plataforma oferece suporte a gestão de desempenho, gestão de configurações, gestão de contabilização, gestão de eventos, gestão de equipamento de rede, gestão de armazenamento, gestão de aplicações, gestão de serviços, gestão de software e gestão de desempenho em rede TCP/IP[1].

Um dos módulos base desta plataforma é o HP *Network Node Manager*, que fornece funcionalidade de gestão de falhas, gestão de configuração e gestão de desempenho em redes TCP/IP.

Para além do *kit* de desenvolvimento, a plataforma inclui um vasto conjunto de aplicações de gestão de redes informáticas, gestão de redes de telecomunicação e gestão de sistemas.

Tivoli NetView

A plataforma de gestão Tivoli NetView foi desenvolvida para máquinas IBM RS/6000, com o sistema operativo AIX, de acordo com a arquitetura de gestão da IBM.

Actualmente a plataforma comporta uma grande variedade de aplicações nativas e aplicações desenvolvidas por terceiros. De entre as funcionalidades de gestão mais relevantes referem-se as seguintes:

- Descoberta dinâmica de rede, com apresentação da topologia lógica;
- Monitorização do desempenho da rede e sistemas, possibilitando uma rápida detecção e isolamento de falhas, e a consequente identificação de problemas;
- Gestão de evento (configuração, filtragem, *logging*);

[1] Termo em inglês, *Transmission Control Protocol/Internet Protocol* (http://searchnetworking.techtarget.com/definition/TCP-IP)

- Segmentação de áreas e responsabilidades de gestão;
- Gestão de inventário;
- Gestão de *trouble tickets*;
- Gestão de relatórios de desempenho, falhas e contabilização, para suporte à análise e planeamento da rede e sistemas; e
- Disponibilidade de interfaces de desenvolvimento.

System Center Configuration Manager

O *System Center Configuration Manager* é uma plataforma centralizada da Microsoft, cujo objectivo principal é possibilitar que os gestores de sistemas possam controlar, a partir de um ponto central, todo o ciclo de vida das infra-estruturas de TI, compreendendo o planeamento, a descoberta, instalação e actualização de sistemas, a distribuição de *software* a servidores, clientes e dispositivos móveis.

As duas vertentes essenciais da plataforma são a gestão das configurações e a gestão da segurança. Como principais áreas funcionais da plataforma referem-se as seguintes:

- Gestão de património, a qual fornece visibilidade sobre o *hardware e software* existentes em toda a infra-estrutura de TI, incluindo informação sobre localização e respectivos utilizadores;
- Distribuição e gestão de actualizações de software, não só para produtos Microsoft, mas também para produtos de terceiros, no que respeita a *drivers* de *hardware, desktop,* computadores portáteis, servidores e dispositivos móveis;
- Gestão de configurações, com particular ênfase nos aspectos de segurança e desempenho de rede; e
- Instalação de sistemas, permitindo a automatização da instalação de servidores clientes, através da rede.

Plataformas *Open Source*

De acordo com Boavida *et all* (2012), para além de vasta gama de plataformas proprietárias, cujas quais algumas foram referidas acima, existem numerosas soluções do tipo *open source*, que se caracterizam por custo zero da plataforma base. Há, no entanto que ter em mente que o custo dessas plataformas não é nulo, já que exigem um investimento inicial na exploração e adaptação da plataforma a realidade que

se pretende gerir, o que se traduz não só na necessidade de pessoal com *know-how* adequado, porêm também num maior tempo para a disponibilização da solução. Para além disso, a falta de suporte ou a necessidade de suporte pago são factores que devem, necessariamente, ser tidos em conta quando se escolhe uma plataforma deste tipo.

Munin

O Munin é uma ferramenta de monitorização, essencialmente virada para a monitorização de desempenho de computadores, redes, serviços e aplicações. Com a ferramenta base ficam imediatamente disponíveis vários *plugins* de monitorização, o que facilita a sua utilização por utilizadores não experientes.

Esta ferramenta caracteriza-se por recolher e memorizar informações sobre uma variedade de nós e serviços, apresentando-a na forma gráfica, através de uma interface web.

O Munin usa a ferramenta RRD, sendo o seu núcleo escrito em Perl. Os *plugins* podem ser escritos numa grande variedade de linguagens de programação. A arquitetura do Munin é do tipo cliente-servidor, em que o servidor executa as funções de recolha e adaptação da informação e os clientes designados por nós executam as funções de agentes de gestão. Toda a informação recolhida é armazena em ficheiros RRD. o Munin possui os seguintes módulos:

- *Munin-update:* é o módulo principal do Munin, fazendo parte do servidor. Este módulo é responsável por contactar os agentes para a recolha de dados e o seu posterior armazenamento;
- *Munin-graph*: é o módulo responsável pela criação dos gráficos a partir da
- informação armazenada nos ficheiros RRD; também faz parte do servidor; e
- *Munin-node*: implementa as funções de agente, correndo nos diversos nós a monitorar.

ZABBIX

O ZABBIX é uma ferramenta moderna, Open Sourse e multiplataforma, livre de custos de licenciamento, pois a sua licença é a GPLv2 (*GNU general Public Licence*[2]). Tem apenas uma versão, que é considerada de classe Enterprise, sendo utilizada para minitorar a disponibilidade e o desenpenho de aplicações,

[2] Termo em inglês, da licença GPLv2 (*http://www.gnu.org/licenses/gpl-2.0.html*).

activos e serviços e rede por todo o mundo (Horst, Pires e Déo, 2015, p. 19).

Toda a informação de gestão é armazenada numa base de dados relacional. O suporte de soluções de comunicação normalizadas é feito através do protocolo SNMP (v1 e v2), possibilitando operações de *polling* e *trap*.

O mecanismo de notificação é extremamente flexível, possibilitando que praticamente qualquer evento gere uma mensagem de alerta, que poderá ser enviada por email.

Como principais características do ZABBIX, referem-se as seguintes:

- Descoberta de dispositivos de rede e servidores;
- Monitorização distribuída, com base em *proxies,* sendo a informação recolhida e disponibilizada num sistema central, acessível via *web*;
- Funcionamento em modo *polling* e possibilidade de geração de *traps*;
- Suporte de mecanismos de autenticação de utilizadores;
- Gestão flexível das permissões dos utilizadores;
- Possibilidade de notificações por *email;*
- Suporte de uma grande variedade de sistemas operativos no servidor (linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X); e
- Suporte de uma grande variedade de agentes, para diversos sistemas operativos (linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X, Tru64/OSF1, Windows).

NAGIOS

O NAGIOS é uma ferramenta de monitorização de sistemas e redes extremamente versátil. Muito da sua versatilidade e potencial advém da sua arquitetura centrada num *daemon* que se encarrega de escalonamento de tarefas de monitorização e de notificação de eventos ao administrador. A monitorização propriamente dita é efectuada por *plugins*, o que confere uma vasta extensibilidade à ferramenta.

Utilizando quer os *plugins* disponíveis com a distribuição base quer *plugins* adicionais, o NAGIOS executa testes a dispositivos e serviços, de acordo com a informação constante do ficheiro de configuração. Os resultados dos testes são armazenados nos ficheiros de *log*. O estado dos equipamentos e serviços é guardado na base de dados de retenção do estado.

A capacidade hierarquia de dispositivos de rede, a definição de dependências, a execução remota de comandos e o desencadeamento de respostas a eventos são características que distinguem o NAGIOS de outros produtos.

Selecção da plataforma de gestão de infraestrutura

Actualmente o mercado oferece plataformas de gestão de redes comerciais e não comerciais, dentre várias destacam-se:

- HP Software & Solutions;
- Tivoli NetView;
- *System Center Configuration Manager;*
- Whatsapp Gold;
- Munin;
- Zabbix;
- NAGIOS; e
- Cacti.

A decisão de empregar uma deles depende das necessidades do administrador da rede.
Aqui é descrita a ferramenta *open source* da ZABBIX que tem os seguintes parâmetros:

- Plataforma *open source*;
- Monitoramento distribuído;
- Monitoramento agregado;
- Monitoramento em tempo real;
- Administração e monitoramento via interface WEB;
- Oferece suporte a SNMP, o que possibilita que a ferramenta possa ser utilizada para monitoria de tráfego mas também qualquer dispositivo com um protocolo SNMP MIB;
- Oferece um mecanismo flexível para a notificação de ocorrências que vão desde email, jabber, sms, whatsapp *aplication*, etc;
- Oferece suporte a mecanismos de autenticação e autorização de utilizadores;

- Apresenta interoperabilidade entre sistemas de diferentes fabricantes;
- Possibilita a adição de agentes para colecta de dados desenvolvidos por terceiros;
- É empregue por uma vasta comunidade, o que facilitaria em termos de suporte; e
- Diferente das outras plataformas levantadas, o ZABBIX permite monitorar na mesma solução, servidores aplicacionais, servidores, equipamentos de comunicação, possibilitando desta forma ter uma solução de monitoria integrada.

Arquitectura do ZABBIX[3]

De acordo com Reis Lima (2004, p. 8), a arquitectura do Zabbix se organiza, dentro do contexto dos serviços de rede, no modelo *three-tier*, que faz uma abordagem em 3 (três) camadas. Essas camadas são: a aplicação, o banco de dados e a interface web. A camada de aplicação é representada pelo *back-end*, responsável por fazer a coleta dos dados activos de rede. A camada de banco de dados é representada pela base de dados, que fica responsável por armazenar as informações coletadas pelo *back-end* e apresentá-las ao *front-end*. Já a camada *interface web* é representada pelo *front-end*, o qual dá acesso a informações para aplicações que utilizam a API do Zabbix.

A figura abaixo, ilusta a arquictetura do Zabbix:

[3] Este titulo foi extraido do capitulo "Apresentacao do Zabbix", de Horst, A. S; Pires, A. S e Déo, A. L. B. (2015). De A a ZABBIX. NOVATEC Editora Ltda.

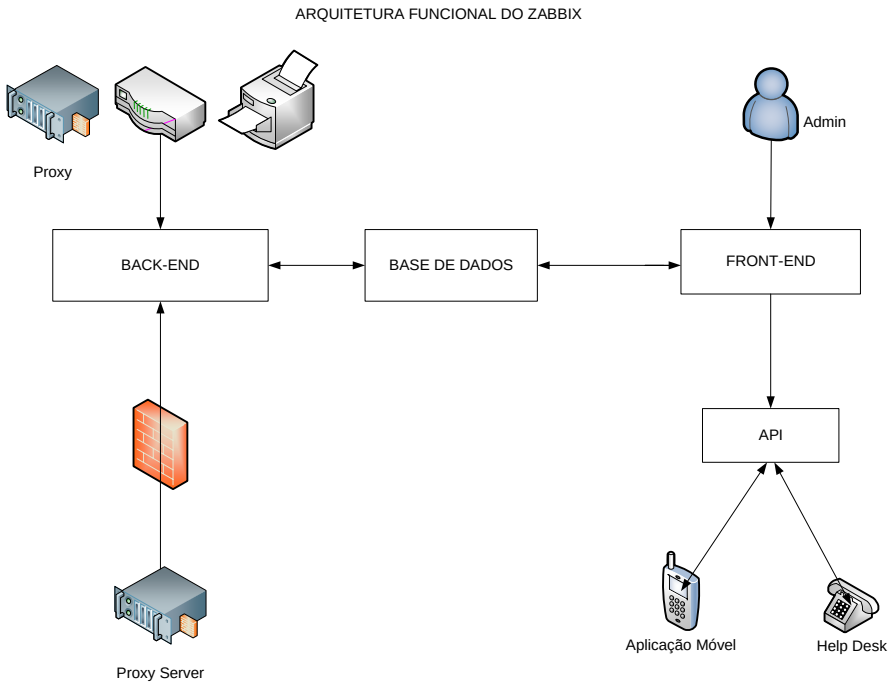

Figura 3.1 – Arquitetura Funcional do Zabbix
Fonte: Reis Lima, J. (2014). Monitoramento de Redes com ZABBIX. BRASPORT Livros e Multimídia Ltda.

Requisitos para instalação

É uma característica, atributo, habilidade ou qualidade que um sistema (ou qualquer um de seus módulos e sub-rotinas) deve necessariamente prover para ser útil a seus usuários.

Requisitos de Hardware

Para instalar o Zabbix existem requisitos de memória (128MB) e de armazenamento (256MB disponíveis em disco). A quantidade de memória e de disco, dependerá da quantidade de *hosts* e de parâmetros monitorados. Se for planeado manter um longo histórico dos parâmetros monitorados deve-se pensar em pelo menos, alguns gigas para ter espaço disponível para uso da base de dados.

Cada processo *deamon* do Zabbix *Server* irá requerer diversas conexões com o servidor de base de dados. A quantidade de memória alocada para cada conexão dependerá das configurações da engine do SGBD[4].

A tabela 3.1 mostra que Zabbix *Server* e especialmente a sua base de dados pode exigir quantidade significativa de recursos da CPU[5] dependendo da quantidade de parâmetros monitorados e da *engine* do

[4] Termo em Inglês, de Sistema de Gestão de Base de Dados
[5] Termo em Inglês, de Unidade Central de Processamento

SGDB.

Plataforma	CPU/Memoria	Base de Dados	Hosts Monitorados
Ubuntu 64	PII 350MHz 256MB	MySQL MyISAM	20
Ubuntu 64	Athlon 3200+ 2GB	MySQL InnoDB	500
Ubuntu 64	Intel Dual Core 6400 4GB	RAID10 MySQL InnoDB ou PostgreSQL	>1000
RedHat Enterprise	Intel Xeon 2xCPU 8GB	Fast RAID10 MySQL InnoDB ou PostgreSQL	>10000

Tabela 3.1 – Requisitos de hardware para instalação do servidor Zabbix

3.1.1. Requisitos de Software

Os requisitos de criação dos binários (arquivos executáveis) necessários para a instalação de um servidor Zabbix ou de um *proxy* Zabbix são muito similares. Basicamente o que muda são os pacotes de banco de dados e de servidor de aplicação (Horst, Pires e Déo, 2015, p. 27).

A tabela abaixo demostra os requisitos especificos do servidor Zabbix:

Grupo	Requisitos
Servidor de aplicação	Apache, versão 1.3.12 ousuperior
Linguagem de programação	A interfce web do Zabbix foi programada em PHP com o uso de algumas bibliotecas opcionais:
	PHP 5.3 ou superior.
	GD2 ou superior.
	libXML 2.6.15 ou superior.
	bcmath, ctype, xmlreader, xmlwriter, TrueType, sessions, sockets, mbstring, gettext, php-xml ou php-dom.

Tabela 3.2 – Requisitos de software para instalação do servidor Zabbix
Fonte: Horst, A. S; Pires, A. S e Déo, A. L. B. (2015). De A a ZABBIX. NOVATEC Editora Ltda.

Requisitos de Base de Dados

O Zabbix deve salvar os dados coletados em algum lugar, então será necessária a escolha de um banco de dados. Ao escolhê-lo, teremos de instalar bibliotecas para acesso, e estas comporão requisito obrigatório para o servidor e para o *proxy* Zabbix (Horst, Pires e Déo, 2015, p. 28).

A tabela abaixo mostra as versões mínimas aceitas para os bancos de dados:

Software	Servidor Zabbix	Proxy Zabbix
MySQl/MariaDB	Versão 5 ou superior	Não recomendado
Oracle	Versão 10g ou superior	Não recomendado
PostgreSQL	Versão 8.1 ou superior	Não recomendado
SQLite	Não recomendado (experimental)	Versão 3.3.5 ou superior
IBM DB2	Versão 9.7 ou superior (experimental)	Não recomendado

Tabela 3.3 – Requisitos de base de dados para a instalação
Fonte: Horst, A. S; Pires, A. S e Déo, A. L. B. (2015). De A a ZABBIX. NOVATEC Editora Ltda.

Processo de instalação do ZABBIX

Como o ZABBIX oferece suporte a vários sistemas operativos, optou-se por instalar a plataforma no sistema operativo Red Hat 7.3, para tal foram seguidos os seguintes procedimentos:

Verificação de dependências

De acordo com Reis Lima (2004, p. 15), dependendo da funcionalidade desejada para o Zabbix Server, tâmbem pode ser necessária a instalação de alguns ou de todos os pacotes, conforme listagem a seguir:

- mysql-devel (bibliotecas e cabeçalhos necessários para acessar o MySQL);
- iksemel-devel (bibliotecas e cabeçalhos necessários para envio de alerta por mensageiro instatâneo);
- net-snmp-devel (bibliotecas e cabeçalhos necessários para monitoramento via SNMP);
- libcurl-devel (bibliotecas e cabeçalhos necessários para monitoramento *web*);
- fping (aplicativo para monitoramento simples);
- libssh2-1-devel (bibliotecas e cabeçalhos necessários para verificação direta via SSH);
- openIPMI-devel (bibliotecas e cabeçalhos necessários para monitoramento de dispositivos por IPMI); e
- openldap-devel (bibliotecas e cabeçalhos necessários para acesso à base de dados LDAP).

Procedimentos de instalação

Instalação do Apache[6], PHP[7] ; e Mysql/MariaDB.

#yum install httpd-devel

#yum install mysql mysql - server

#yum install php php-cli php-common php-devel php-pear php-gd php-mbsrting php-mysql php-xml

[6] Termo em inglês, Apache (https://httpd.apache.org/)
[7] Termo em inglês, PHP (http://www.php.net/)

#service httpd start

#service mysql start

#mysql_secure_installation

Configuração do *Yum Repository*

#rpm -Uvh http://repo.zabbix.com/zabbix/2.4/rhel/6/x86_64/zabbix-release- 2.4-1.el6.noarch.rpm

Instalação do ZABBIX *Packages*

#yum install zabbix-server zabbix-web zabbix zabbix-agent zabbix-java-gateway -y

#yum install zabbix-server-mysql zabbix-web-mysql -y

#rpm -qa | grep zabbix

Configuração do Zabbix *Apache File*

#vi /etc/httpd/conf.d/zabbix.conf php_value

max_execution_time 300

php_value memory_limit 128M php_value

post_max_size 16M php_value

upload_max_filesize 2M php_value

max_input_time 300

php value date.timezone Africa/Maputo

```
#service http restart
```

Criação da base de dados para o ZABBIX

```
#mysql -u       root -p

mysql> create database zabbix character set utf8;

mysql> grant all privileges on zabbix.* to 'zabbix'@'localhost' identified by 'zabbix';

mysql> flush privileges; mysql>

quit

#mysql -u zabbix -p zabbix < /usr/share/zabbix-mysql/schema.sql

#mysql -u zabbix -p zabbix < /usr/share/zabbix-mysql/images.sql

#mysql -u zabbix -p zabbix < /usr/share/zabbix-mysql/data.sql
```

Start* Zabbix *Server

```
#service zabbix-server start

#service zabbix-server status

#ps -ef | grep zabbix

#netstat       -nat | grep 10051
```

Após a realização destes 6 (seis) procedimentos a instalação está concluída, faltando somente aceder a plataforma e parametriza-la. Para tal no *web browser* digita-se o seguinte endereço: http://endereco_da_estacao/zabbix

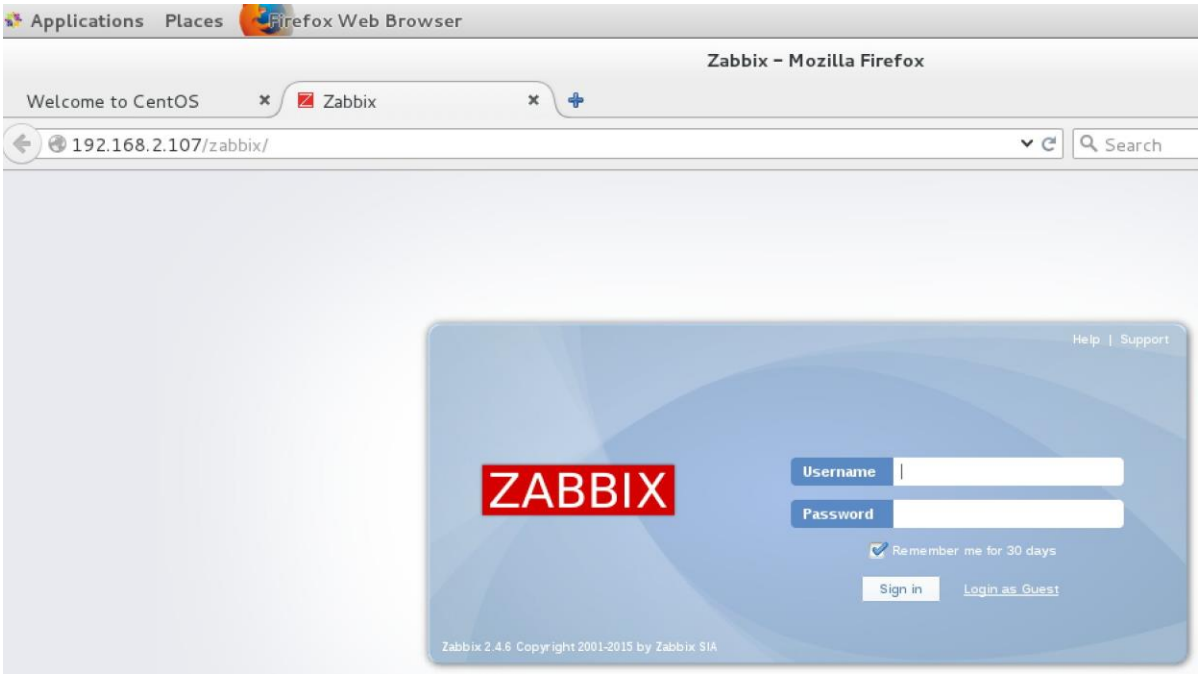

Figura 3.2 – Formulário de autenticação do ZABBIX

Configuração de autenticação do ZABBIX

username:admin

password:zabbix

***Troubleshooting* do ZABBIX**

#vi /etc/zabbix/zabbix-server.conf

DBName=zabbix

DBUser=zabbix

DBPassword=zabbix

#service zabbix-server restart

Monitoria de aplicações informática através do ZABBIX

Após instalar o ZABBIX como ferramenta de gestão de redes, já se torna possível efectuar a monitoria da infraestrutura tecnológica que foi um dos propósitos que motivou este estudo.

A monitoria de aplicações pode ser realizada de diversas maneiras, no presente estudo optou- se por utilizar o zapcat que é um pacote java que é feito o seu *deploy*[8] em um servidor aplicacional, no presente utilizou-se JBOSS. O zapcat oferece uma *interface Web* onde se pode visualizar os Itens suportados para o monitoramento e um agente ZABBIX que funciona dentro do JBOSS.

Este agente funciona numa porta diferente da do agente padrão do Zabbix, funciona na porta 10052 ao invés da porta usual do agente Zabbix que é a 10050.

O zapcat provê compatibilidade entre itens criados e os item padrão utilizando o agente Zabbix, exceto as chaves que serão utilizadas no item.

Template

Segundo Horst, Pires e Déo (2015, p. 87), um dos recursos que dá mais agilidade ao Zabbix é o recurso de *tempalte*. Várias ferramentas suportam esta funcionalidade, entretanto o Zabbix é uma das poucas que suporta o recurso em conjunto com herança de propiedades. Mas o que é este tal de template? Para que serve?

A infopédia[9] define *template* como sendo: "Ambiente estabelecido como modelo, permitindo criar conteúdos de uma forma rapida". Para a monitorização usando o Zabbix, *template* é um modelo de regras de coleta, aleratas e representações gráficas que podem ser aplicadas facilmente a elementos monitorados.

No entanto Reis Lima (2014, p. 47), com a utilização de templates, tudo acontece por herança, ou seja, um host pode estar associado a vários templates, que tâmbem podem estar associados a outros templates. Com isso, todos objectos, como itens, gráficos, triggers, entre outros, serão herdados e associados ao host em questão.

Alertar (Notificações)

O Zabbix utiliza vários métodos para notificar os eventos ocorridos, tais como: envio de e-mail, SMS,

[8] http://whatis.techtarget.com/definition/deploy
[9] *http://www.infopedia.pt/lingua-portuguesa/Template.*

mensagem via chat etc. Também é possivel utilizar a função de reconhecimento de eventos, na qual o Zabbix pode escalonar esses eventos para notificar várias pessoas em um determinado periodo de tempo. Um exemplo seria executar um comando remoto um minuto após identificar um problema no servidor web. Se após dez minutos o problema persistir, o sistema envia um e-mail e uma mensagem SMS para o administrador de rede (Reis Lima, 2014, p. 49).

Configuração de alertas de e-mail

Após o ZABBIX estar configurado para monitorar aplicações ou dispositivos, é necessário configurar os mecanismos de alerta. Estes servirão para informar ao administrador da rede sobre estado da rede e/ou aplicações.

Procedimentos para instalação

1ª ETAPA: configuração do *postfix*

yum install cyrus-sasl cyrus-sasl-devel cyrus-sasl-gssapi cyrus-sasl-md5 cyrus-sasl-plain mutt postfix Em seguida, deve-se aceder o diretório de configuração do *Postfix* e efectuar o *backup*[10] do arquivo de configuração:

```
# cd /etc/postfix/

# mv main.cf main.cf.old
```

Após efetuar o *backup* cria-se um novo arquivo de configuração para *postfix*:

```
# vi main.cf
```

No arquivo criado coloca-se as seguintes linhas:

```
#SMTP relayhost

relayhost = [smtp.gmail.com]:587
```

[10] Termo inglês que tem o significado de Cópia de Segurança

TLS Settings smtp_tls_loglevel = 1

smtp_use_tls = yes

smtpd_tls_received_header=yes

TLS

smtp_sasl_auth_enable = yes

smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd

smtp_sasl_security_options = noanonymous

smtp_sasl_tls_security_options = noanonymous

Na linha relayhost = [smtp.gmail.com]:587, fez-se menção ao gmail, no entanto é possível referenciar outro servidor de email.

Após introduzir as linhas acima, cria-se o arquivo "sasl_passwd", contendo o servidor SMTP e a conta que será utilizada para envio dos e-mails.

vi sasl_passwd

[smtp.gmail.com]:587 Conta_email@gmail.com:Senha

Em seguida, executa-se o comando "postmap" no arquivo "sasl_passwd" e no "main.cf", para que eles possam ser reconhecidos e utilizados pelo *postfix*:

postmap /etc/postfix/sasl_passwd; postmap /etc/postfix/main.cf

Executada a instrução acima, reinicia-se o serviço do postfix:

service postfix restart

Desta forma o servidor está preparado para o envio de emails.

Visualizar

A ultima função básica que temos é a visulalização de alto nível que o Zabbix oferece, onde podemos ver alertas através de um painel de controle. Também podemos visualizar os dados coletados através de gráficos, mapas ou telas.

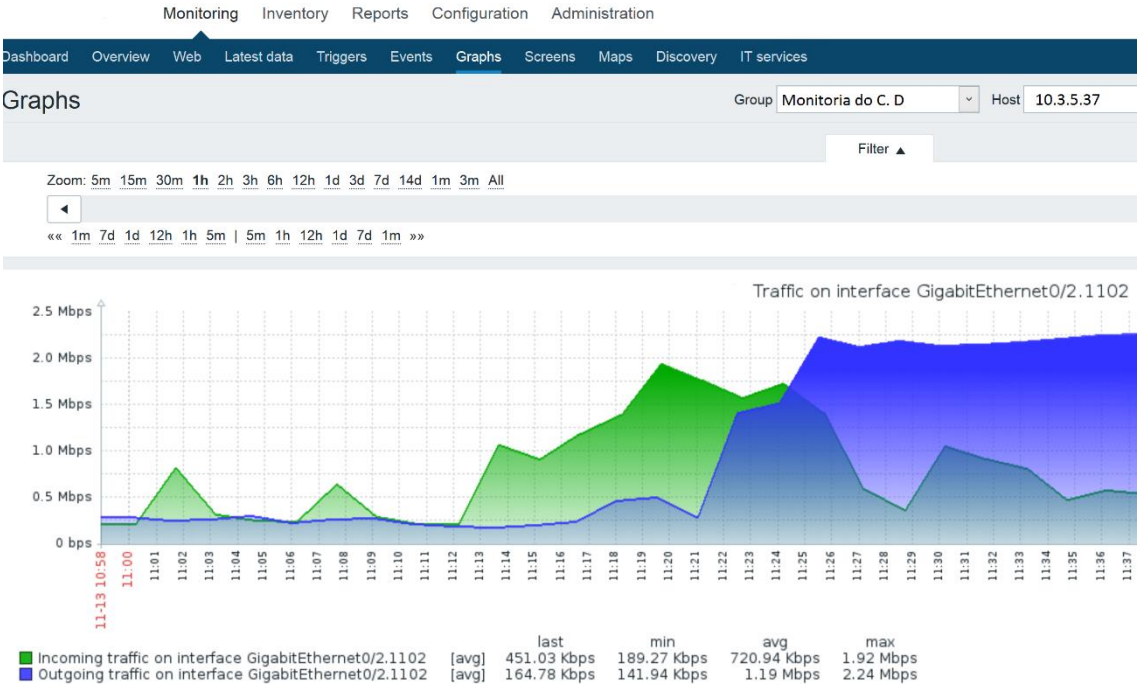

Figura 3.3 – Gráfico de um item de rede