PROJETO DE REDES
www.projetoderedes.com.br

GERENCIAMENTO E MONITORAÇÃO DE REDES DE COMPUTADORES UTILIZANDO-SE ZABBIX

ESLEY BONOMO

2006

ESLEY BONOMO

GERENCIAMENTO E MONITORAÇÃO DE REDES DE COMPUTADORES UTILIZANDO-SE ZABBIX

Monografia apresentada ao Departamento de Pós Graduação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-Graduação *Lato Sensu* em Administração de Redes Linux, para a obtenção do título de especialista em Administração de Redes Linux.

Orientador
Joaquim Quinteiro Uchôa

LAVRAS
MINAS GERAIS – BRASIL
2006

ESLEY BONOMO

GERENCIAMENTO E MONITORAÇÃO DE REDES DE COMPUTADORES UTILIZANDO-SE ZABBIX

Monografia apresentada ao Departamento de Pós Graduação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-Graduação *Lato Sensu* em Administração de Redes Linux, para a obtenção do título de especialista em Administração de Redes Linux.

APROVADA em 30 de abril de 2006

Prof. Denilson Vedoveto Martins

Profa. Simone Markenson Pech

Joaquim Quinteiro Uchôa
(Orientador)
LAVRAS
MINAS GERAIS – BRASIL

Principalmente a minha esposa, pelo amor, carinho, compreensão e paciência.
À minha família pelo carinho, amizade e por ter me dado a oportunidade de estar aqui hoje.

Agradecimentos

Agradeço primeiramente a Deus, pois sem ele nada disso teria acontecido.

Depois minha esposa pelo apoio em tudo para que este trabalho fosse concluído, inclusive ao tempo doado sem a minha companhia.

Aos meus cunhados por terem me convencido a fazer a defesa da monografia no momento em que já tinha desistido.

Resumo

Nos dias atuais ouve-se muito falar em segurança de redes, hackers, vírus, Spywares, etc. Sem tirar o mérito da importância da segurança de redes, mas poucas pessoas se dão conta do quão é importante ter um maior controle interno da rede referente a planejamento de capacidade, dados sobre tráfego, informações de desempenho e notificações de erros.

A proposta deste trabalho é estudar uma ferramenta que atue nas áreas da “Gerência de Rede” auxiliando o administrador a obter mais informações necessárias para manter o bom funcionamento da rede minimizando o problema de falta de controle em um ambiente computacional.

A ferramenta escolhida para ser usada como auxilio ao administrador é o ZABBIX, pois disponibiliza de inúmeros recurso na ajuda da administração de rede, como gráficos de maior desempenho na coleta dos dados em tempo real e com mais informações, alertas de erros ocorridos nas entidades gerenciadas, configurações, auditoria dos dados, etc. Então o que será visto deste trabalho é a implantação e configuração de uma poderosa ferramenta usada para o gerenciamento e monitoração de redes de computadores.

Sumário

Lista de Figuras

1 – Introdução

Há alguns anos que o crescimento de redes de computador tem tido uma atenção especial, pois cada vez mais pessoas usam computadores com acesso à internet. Cada vez mais as empresas são dependentes de computadores para a execução de suas atividades, tendo a necessidade de um acesso global para melhor comunicação com seus clientes e/ou parceiros. E com isso as redes de computadores (LANS e WANS) vêm crescendo de forma muito rápida ao ponto de ser necessário ter um melhor controle sobre seus recursos.

É muito grande a necessidade de uma plataforma que tenha um controle unificado sobre os processos e recursos utilizados na rede para atender da melhor maneira possível às necessidades de seus clientes. Para isso, é necessário saber a quantidade de memória utilizada pelos processos, bem como a carga de cada processo sobre o processador. Além disso, é importante verificar se a rede está com um tráfego intenso de informações ocasionando um congestionamento e com isso uma demora nas respostas aos pedidos solicitados pelos clientes. O uso desse tipo de ferramenta iria auxiliar os administradores de rede a distribuir melhor o tráfego e a carga de processamento dos servidores. Além disso, facilitaria a identificação de ocorrência de falhas nas entidades que estão sendo gerenciadas tendo uma visão integral da rede.

A proposta deste trabalho é o estudo da ferramenta ZABBIX, que é uma plataforma unificada de Monitoramento de Redes capaz de ajudar um administrador a solucionar grande parte dos problemas encontrados nas redes, de forma mais eficiente e eficaz. Além disso este trabalho, irá auxiliar os administradores de Redes na escolha de uma ferramenta capaz de ajudar-lhe com suas atividades de monitoramento e gerenciamento de redes. Para isso, o texto encontra-se organizado como se segue: no Capítulo 2 será visto uma referência teórica das áreas envolvidas para que esta ferramenta seja compreendida não somente pela sua praticidade, mas também pela parte teórica. No Capítulo 3 serão apresentadas algumas informações sobre o ZABBIX, no que ele poderá ser usado, por quem, requisitos e instalação. Já no Capítulo 4 será mostrado como configurar e utilizar o ZABBIX para um ambiente básico de teste, como o usado neste trabalho como estudo de caso. No capítulo 5, por fim serão apresentadas as principais conclusões do trabalho e a perspectiva de trabalhos futuros.

2 – Referencial Teórico

2.1 – Gerência de Redes

A Gerência de redes está associada ao bom funcionamento da rede, bem como o meio físico propriamente dito e seus recursos de hardware. E para isto existem cinco áreas, como ilustrado na Figura 1, que são responsáveis por uma determinada função. São elas:

- A **gerência de configuração** é responsável pela descoberta, manutenção e monitoração de mudanças à estrutura física e lógica da rede. As funções básicas desta área de gerência são: coleta de informações sobre a configuração, geração de eventos, atribuição de valores iniciais aos parâmetros dos elementos gerenciados, registro de informações, alteração de configuração dos elementos gerenciados, início e encerramento de operação dos elementos gerenciados [Oda94].
- A **gerência de falhas** é responsável pela detecção, isolamento e conserto de falhas na rede. As funções básicas são: detecção, isolamento e antecipação de falhas, supervisão de alarmes, re-estabelecimento dos elementos com problemas,

testes, registro de ocorrência e emissão de relatórios para análise [Oda94] e [Cis99].

- A **gerência de desempenho** que é responsável pela monitoração e análise do desempenho e planejamento de capacidade. Esta área de gerência deve selecionar os indicadores de desempenho, monitorar e analisar o desempenho, planejar a capacidade e alterar o modo de operação [Bri93] e [Her94].
- A **gerência de segurança** é responsável pela proteção dos elementos da rede, monitorando e detectando violações de política de segurança estabelecida. Esta área de gerência preocupa-se com a criação, monitoração e manutenção de serviços de segurança e com a manutenção de *logs* de segurança [Cis99].
- A **gerência de contabilidade** é responsável pela contabilização e verificação de limites da utilização de recursos da rede, com a divisão de contas feita por usuários ou grupos de usuários. As funções básicas são: a coleta de informações sobre a utilização, o estabelecimento de cotas de utilização e escala de tarifação, e a aplicação de tarifas e faturamento.

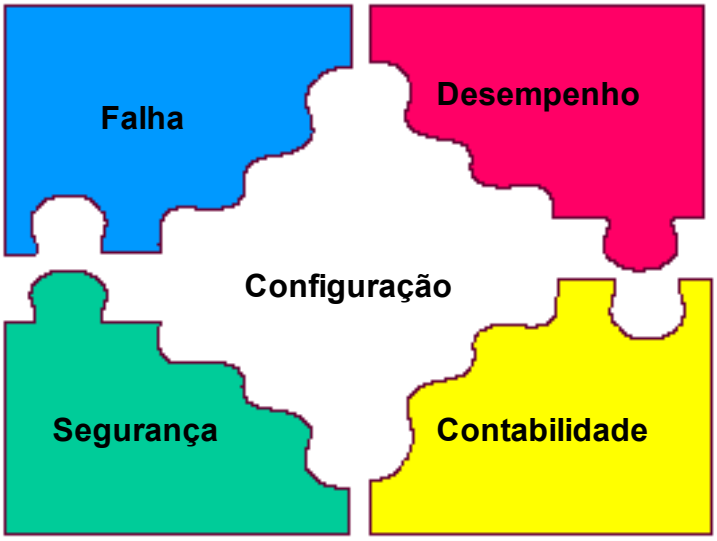


Figura 1: Áreas da Gerência de Rede

2.1.1 – Agentes e Gerentes

Toda aplicação de Gerência de Redes é baseada na troca de informações entre um agente e um gerente, sendo que cada um possui as seguintes características:

- **Agente**: Coleta informações relativas ao funcionamento dos objetos que gerencia e armazena essas informações na MIB e realiza operações de gerenciamento sobre estes objetos atendendo a solicitações enviadas pelo gerente, ou até mesmo envia informações sem a solicitação no caso de falhas.

- **Gerente**: Também conhecido como NMS (*Network Management Stations*) coleta informações sobre os objetos gerenciados junto aos agentes, processa as informações e solicita aos agentes que execute as funções de gerenciamento a fim de controlar o funcionamento do objeto gerenciado.

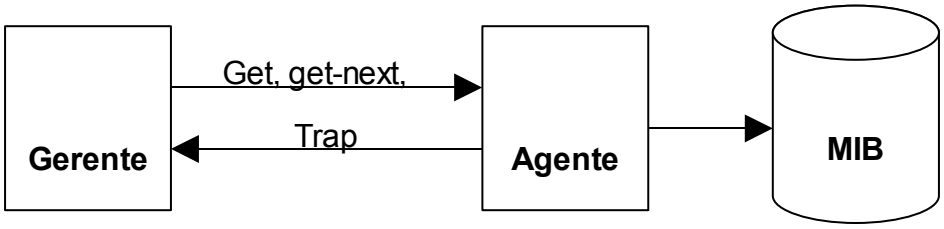


Figura 2: Conceito de Gerente e Agente

Como pode ser visto na Figura 2, o agente e gerente se comunicam através de operações e notificações definidas no protocolo. O protocolo trabalhado neste texto é o SNMP (*Simple Network Management Protocol*).

As informações sobre objetos gerenciados são armazenadas na MIB, que contém informações sobre o funcionamento do host, dos gateways e dos processos que executam os protocolos de comunicação (IP, TCP, ARP, etc). A MIB é especificada na ASN.1[1]. O funcionamento do SNMP baseia-se em troca de operações que permitem que o gerente solicite que

1 Do inglês *Abstract Sintax Notation.1*. Permite a transferência de grandes inteiros, sem desperdiçar espaço em cada transferência, usa uma combinação de tamanho e valor para cada objeto a ser transferido.

o agente lhe informe, ou modifique, o valor de uma variável de um objeto da MIB. O SNMP define também uma operação que permite ao agente informar o gerente da ocorrência de um evento específico.

2.2 – SNMP (*Simple Network Management Protocol*)

Ao longo dos anos, o SNMP vem sendo usado como o principal protocolo no gerenciamento de rede. E o sucesso deste protocolo é tão grande, que ele não é somente usado para gerenciamento de equipamentos tradicionais de rede como computadores, roteadores, etc. Atualmente, qualquer equipamento que tenha a necessidade de estar 100% em funcionamento e condizente com as perspectivas de mercado, deve ter incorporado à capacidade de permitir ser gerenciado via SNMP. E essa tendência, faz com que os mais variados equipamentos já saiam com suporte ao SNMP de fábrica para estar na realidade de mercado, como por exemplo: Modem ADSL, Impressoras e etc.

Como o próprio nome do protocolo diz “simples”, ele ganhou fama pela facilidade em implementação de soluções com o seu uso. Quando o modelo RM-OSI (*Reference Model – Open System Interconnection*) ficou pronto em 1993, após um cuidadoso e demorado desenvolvimento, o SNMP já estava difundido em diversos produtos.

O sistema de gerenciamento de rede da arquitetura TCP/IP opera na camada da aplicação e baseia-se no protocolo SNMP. Os padrões que definem a estrutura de gerenciamento de redes Internet são descritos nos documentos RFC-1155 [R1155], RFC-1156 (MIB – *Management Information Base*) [R1156] e RFC-1157 (SNMP - *Simple Network Management Protocol*) [R1157]. Como no esquema de gerenciamento OSI, os processos que implementam as funções de gerenciamento Internet atuam como agentes e gerentes, como visto no item 2.1.1.

2.2.1 – Versões SNMP e RFCs

A IETF (*Internet Engineering Task Force*) é responsável pela definição dos protocolos que controlam o tráfego da internet, incluindo o SNMP. Ela é quem publica os RFCs (*Request for Comments*), que são especificações para os diversos protocolos existentes no mundo IP. Primeiramente, os documentos se submetem ao rastreamento de padrões como padrões sugeridos, depois passam para o status de *draft* final é ocasionalmente aprovada, a RFC recebe o status *Standard* (padrão).

Duas outras designações de rastreamento de padrões, histórico e *experimental*, definem, respectivamente, um documento substituído por uma RFC mais recente e um documento que ainda não está pronto para se tornar um padrão. A

seguir temos uma lista que engloba todas as versões atuais do SNMP e o status emitido pela IETF para cada uma.

- *SNMP Version 1* (SNMPv1) – é a versão padrão atual do protocolo SNMP, definida na RFC 1157 [R1157] e é um padrão completo da IETF. A segurança do SNMPv1 baseia-se em *comunidades*, que não são nada mais do que senha: *string* de texto puro que permitem que qualquer aplicativo baseado em SNMP, que reconheça a *string*, tenha acesso a informações de gerenciamento de um dispositivo. Geralmente existem três comunidades no SNMPv1: *read-only*, *read-write* e *trap*.
- *SNMP Version 2* (SNMPv2) – é frequentemente citado como SNMPv2 baseado em *string* de comunidade. Essa versão tem a denominação técnica de SNMPv2c. Ela está definida na RFC-1905 [R1905], RFC-1906 [R1906] e RFC 1907 [R1907].
- *SNMP Version 3* (SNMPv3) – é a última versão do protocolo a alcançar o status completo da IETF. Está definido na RFC-1905 [R1905], RFC-1906 [R1906], RFC-1907 [R1907], RFC-2571 [R2571], RFC-2572 [R2572], RFC-2573 [R2573], RFC-2574 [R2574] e RFC-2575 [R2575], que inclui suporte

para autenticação rigorosa e comunicação privativa entre as entidades gerenciadas.

2.2.2 - Operações do SNMP

O SNMP por si só é um protocolo de requisição/resposta simples. Os NMS (*Network Management Systems*) podem enviar múltiplas requisições sem receber uma resposta. Quatro operações básicas são definidas no SNMPv1:

- O ***get*** permite que o NMS recupere uma instância de um objeto gerenciado de um agente.
- O ***get-next*** permite que o NMS recupere a próxima instância de objetos de uma tabela ou lista em um agente. Se o NMS quiser recuperar todos os elementos de uma tabela de um agente, ele inicia com uma operação *get* seguida de uma série de operações *get-next*.
- O ***set*** permite que o NMS modifique valores de uma instância de objetos gerenciados em um agente.
- E o ***trap*** é usado pelo agente para informar o NMS sobre algum evento ocorrido como, por exemplo, um erro.

Há também as operações *get-bulk*, *notification*, *inform* e *report* que não serão abordados nesta subseção.

2.2.3 – Formato das Mensagens

Os pacotes de mensagem do SNMP são divididos em duas partes. A primeira parte contém a versão e o nome da comunidade. A segunda parte contém o protocolo da unidade de dados (PDU) do SNMP especificando a operação que será realizada e a instância de objetos envolvida na operação. A Figura 3 ilustra o formato das mensagens SNMP.

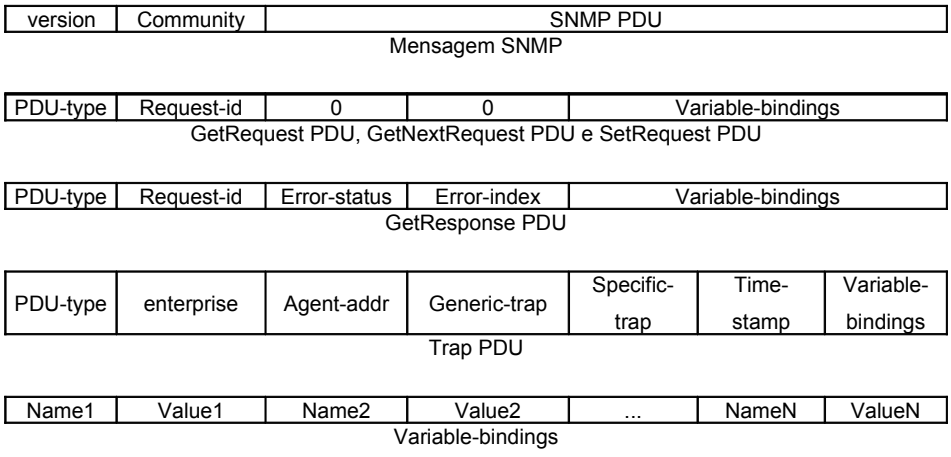


Figura 3: Formato das mensagens SNMP

2.3 – MIB

A MIB (*Management Information Base*) pode ser considerada um banco de dados de objetos gerenciados que o agente rastreia, ou seja, é a definição dos próprios objetos. Todo tipo de informação sobre os estados e estatísticas acessados pelo NMS é definida em uma MIB.

Um agente pode implementar várias MIBs, porém todos os agentes implementam uma MIB específica denominada MIB-II (RFC 1213) [R1213]. Esse padrão define variáveis para elementos como dados estatísticos de uma interface, assim alguns outros aspectos relacionados ao próprio sistema. O principal objetivo da MIB-II é fornecer informações gerais sobre gerenciamento de TCP/IP e não engloba todo item possível que um fornecedor gerenciaria em um dispositivo especifico [Mau01].

3 – ZABBIX

ZABBIX[2] é um *software*, distribuído sob a licença GPL, que monitora um vasto número de parâmetros de rede e o perfeito funcionamento dos servidores. ZABBIX usa um flexível mecanismo de alarmes que permite aos usuários configurar um *e-mail* para receber um alerta de algum evento que ocorra com os mecanismos gerenciados. Isso permite uma fácil resolução do problema encontrado nos servidores. O criador Alexei Vladishev

2 Mais informações sobre o ZABBIX podem ser encontradas em http://www.zabbix.org.

pensou em unificar em uma única ferramenta soluções de monitoramento sem alto custo permitindo o monitoramento em tempo integral.

ZABBIX oferece excelentes características de relatórios e visualização de dados armazenados. Isso faz o ZABBIX ideal para o planejamento de capacidade. ZABBIX suporta *polling* (forma de capturar dados de tempo em tempo) e *trapping* (notificação de alarmes). Todos os relatórios e estatísticas do ZABBIX, bem como as configurações dos parâmetros são acessadas através de uma interface gráfica na *web*. E esta interface assegura os estados de bom funcionamento da rede e de seus servidores possam ser acessados de qualquer lugar. Propriamente configurado ZABBIX pode ter um papel importante em monitorar toda a infraestrutura de TI. Isso é igualmente verdadeiro para pequenas companhias com poucos servidores e para grandes companhias com grandes números de servidores. O ZABBIX oferece:

- Suporte para ambos mecanismos de *polling* e *trapping*;
- Servidores para Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X;
- Agentes de alta performance nativos;
- Monitoramento de servidores sem um agente instalado;
- Autenticação de usuário segura utilizando criptografia dos dados;
- Permissões de usuários flexíveis;

– Interface gráfica w*eb*;

– Flexível notificação e predefinidos eventos por e-mail;

– Alto Nível de visualização (Negócios) de recursos monitorados.

A utilização do ZABBIX traz ao administrador alguns benefícios indispensáveis nos dias de hoje, como:

– Solução de Código aberto;

– Alta eficiência para agentes baseados nas plataformas UNIX e WIN32;

– Baixa curva de aprendizado;

– Alto retorno de investimento através dos dados coletados, diminuindo o tempo gasto com soluções erradas dos problemas;

– Baixo custo de implantação pois é de fácil instalação;

– Muito simples de configurar;

– Sistema de monitoramento centralizado. Todas informações (configuração, dados de performance) são armazenadas em uma base de dados relacional;

– Serviço de árvore de alto nível;

– Instalação muito fácil;

– Suporte para o SNMP (v1, v2). Ambos aceitam polling e trapping;

– Visualização de capacidades;

– Procedimento interno de tarefas proprietárias.

3.1 – Características do ZABBIX

Como foi visto no item 2.1, um sistema de gerência de redes possui algumas funções básicas para tratar as áreas da gerência. Então baseando-se nestas funções, o ZABBIX possui as seguintes características:

3.1.1 – Monitoramento de Desempenho

Um dos mais importantes usos do ZABBIX é o monitoramento de desempenho. Carga do processador, número de processos rodando, número de processos, atividade no disco rígido, espaço da memória *swap* e disponibilidade da memória são alguns de inúmeros parâmetros de sistemas que o ZABBIX é capaz de monitorar. O ZABBIX prove ao administrador de sistemas informações em tempo real sobre o desempenho de um servidor. Além disso, ZABBIX pode produzir gráficos de tendências para ajudar na identificação de gargalo no desempenho do sistema. Os gráficos gerados pelo ZABBIX são

mais eficientes em se comparando com o NAGIOS, por exemplo, pois utilizam o pacote *RRDTool*[3], em vez do *MRTG*[4].

3.1.2 – Mecanismo de Alerta

Ter o monitoramento de desempenho em um sistema é muito bom, mas ele seria pouco usado sem o poderoso mecanismo de notificação. Com o ZABBIX, um administrador pode definir virtualmente uma possível condição para um gatilho, usando flexíveis expressões. Em algum momento quando essas condições forem verdadeiras (ou falsas), um alerta será enviado por *e-mail* para um endereço definido pelo administrador. Programas externos podem ser usados para notificar o usuário como SMS, notificação por celular, etc.

ZABBIX pode adivinhar comportamentos futuros de parâmetros monitorados usando um Algoritmo do Mínimo Quadrado. Isso permite o usuário ser notificado bem antes de o estado do sistema alcançar o nível crítico.

3 RRDTool (Round Robin Database Tool) é uma ferramenta poderosa para monitoração de tráfego, que reduz sensivelmente a carga gerada pela monitoração para a exibição dos gráficos, o que possibilita uma representação visual em tempo real do tráfego.

4 MRTG (Multi Router Traffic Grapher) é outra ferramenta para monitoração de tráfego. Ela gera um relatório que é exibido em HTML com imagens.

3.1.3 – Monitoramento de arquivos de *logs*

O ZABBIX pode ser usado para o monitoramento de arquivos de *logs*. Como por exemplo, quando algum valor for impresso em um determinado arquivo de *log*, ele poderá disparar um alerta para o Administrador.

3.1.4 – Verificação de Integridade

ZABBIX é capaz de verificar a integridade do servidor. Todos arquivos de configuração críticos, binários, *kernel*, *scripts* e páginas HTML de servidores *web* podem ser monitorados permitindo que o administrador possa ser alertado toda vez que um desses arquivos forem alterados.

3.1.5 – Serviços de Auditoria

Todos valores dos parâmetros monitorados são armazenados em banco de dados. Os dados coletados podem ser usados mais tarde para algum propósito. O ZABBIX gera uma auditoria das mudanças dos valores dos parâmetros para que o administrador possa saber quem as fez, para em caso de algum problema possa tentar identificar os culpados.

3.1.6 – Capacidade de Planejamento

Observando tendência de carga de processos, uso de disco rígido, atividade de banco de dados ou outras medidas importantes, o ZABBIX permite ao administrador de sistemas uma visão clara para uma necessidade futura de atualização de um *hardware* específico, quando o mesmo estiver sobrecarregado.

3.1.7 – Monitoramento do SLA

ZABBIX é capaz de monitorar Serviços ao Nível de Contrato (*Service Level Agreements* - SLA). Mantém também SLA - os dados históricos relacionados que ajudam identificar e melhorar áreas fracas de um infraestrutura de tecnologia de informação.

3.1.8 – Visualização de alto nível dos recursos e serviços de TI.

Uma escala de serviços de alto nível permite a criação de dependências entre vários recursos de tecnologia de informação. Tal representação permite as seguintes questões serem respondidas:

Quais os serviços de TI dependem da disponibilidade dos recursos X?

Exemplo: Se a carga do processador está muito alta no servidor A, então estes serviços de TI poderão ser afetados: Servidor Oracle, Banco via *web*, Processamento de transações *online* e etc.

Quais os recursos específicos um serviço de TI depende?

Exemplo: Um portal WEB deve depender dos seguintes recursos:

1. Carga do processador no servidor A
2. Provedor de serviço internet (ISP) para conexão
3. Espaço de disco no servidor A
4. Disponibilidade do banco de dados Oracle no servidor B
5. Velocidade de execução das requisições dos usuários
6. Disponibilidade do servidor Apache no servidor C
7. etc

Tais níveis de dependência ajudam a identificar pontos fracos na infraestrutura de TI.

Exemplo: Se diversos serviços críticos oferecidos pelo departamento de TI dependerem de, por exemplo, disponibilidade de espaço em disco para alguns servidores, então é tempo de pensar sobre a distribuição de volume de carga de diferentes servidores ou preparar o disco para eliminar possíveis riscos.

3.1.9 – Outros

Outra característica do sistema está relacionada em permitir a Análise da Disponibilidade, ou seja, quando um determinado servidor gerenciado possa ter ficado indisponível para uso. Além disso a Representação Gráfica de Informações Coletadas pode ser usada para tomar decisões, pois são mostrados em formas de relatórios. Outro ponto é a forma de mostrar os elementos gerenciados ou não em forma de Mapas de Redes permitindo assim uma melhor visão da rede. Mais uma característica interessante é a Personalização de Telas, que permite ao administrador definir o formato de suas telas, ou seja, quais dados, gráficos e mapas poderão ser vistos.

3.2 – Requisitos

3.2.1 – Requisitos de Hardware

Para a instalação do ZABBIX há a necessidade mínima de ter 32 Mb de memória física e 20 Mb de espaço em disco. Porém, o número exato de memória e espaço em disco requeridos dependerão do número de *hosts* e parâmetros que serão monitorados. Se for planejado um longo histórico de parâmetros monitorados, pode-se prever que o banco de dados ocupará *gibabytes* de espaço em disco.

Cada processo do ZABBIX requer um número grande de conexões com o servidor. Uma quantidade de memória alocada para as conexões depende da configuração do banco de dados. É importante ressaltar que quanto mais memória física a máquina estiver, mais rápido será o banco de dados, e consequentemente o ZABBIX.

3.2.2 – Plataforma suportadas

Devido a necessidade de segurança e a critica missão natural de monitoramento de servidores, UNIX é o único sistema operacional que pode consistentemente responder ao desempenho necessário, tolerância de falha e auto recuperação. ZABBIX opera sobre versões principais do mercado. ZABBIX é testado nas seguintes plataformas:

- Linux 2.xx
- Solaris 2.xx
- HP-UX 11.xx
- AIX 4.3
- Free BSD 4.3
- SCO Open Server 5.0.5
- Mac OS/X

Pelo fato de o ZABBIX ter sido testado somente para os sistemas mencionados acima, nada impede de funcionar também em outros sistemas operacionais baseados em UNIX.

3.2.3 – Requisitos de *Software*

ZABBIX é construído em cima do servidor WEB Apache, banco de dados MySQL ou PostgreSQL e a linguagem de *script* PHP. A seguir estão os aplicativos que são requisitos para rodar o ZABBIX:

– **Apache**: Versão 1.3.12 ou maior. O apache pode ser encontrado em http://www.apache.org.

– **MySQL (ou PostgreSQL)**: Versão 3.22 ou maior. O MySQL pode ser encontrado em http://www.mysql.com.

– **PostgreSQL (ou MySQL)**: Versão 7.0.2 ou maior: PostgreSQL pode ser encontrado em http://www.postgresql.org.

– Arquivos de desenvolvimento para MySQL ou PostgreeSQL, normalmente encontrados como parte dos pacotes *mysql-dev* ou *postgresql-dev*.

– **PHP**: Versão 4.0 ou maior. PHP é um modulo encontrado em http://www.php.net. PHP deve ser compilado com o módulo do Apache. PHP 5.0 é suportado também.

– **Módulo PHP GD ou GD2**: O módulo é requerido para mostrar mapas e gráficos. O módlo suporta imagens no formato PNG.

– **Módulo PHP 4.0 MySQL ou PostgreSQL**

– **GNU Make**: Necessário para criar o ZABBIX ou seus agentes. No caso de ser usado versões pré-criadas, GNU *make* não será necessário.

– **Navegador *Web***: No lado do cliente e que suporte páginas HTML e imagens PNG.

3.3 – Componentes do ZABBIX

O ZABBIX consiste de diversos componentes de software e a responsabilidade de cada um está descrita a seguir:

– **Servidor ZABBIX**: Esse é o centro do software ZABBIX. O servidor pode remotamente verificar serviços de redes (como um servidor *web* ou um servidor de *e-mail*) usando simplesmente a verificação do serviço, mas é também o repositório central onde toda configuração, estático e operacional são armazenadas. Além disso é a entidade do ZABBIX que irá ativar o alerta ao administrador do sistema toda vez que um problema aparecer em algum sistema monitorado.

– **Agente ZABBIX:** para monitorar recursos locais e aplicações (tais como HD, memória, estatística de processador) em sistemas na rede, esses sistemas devem rodar o agente ZABBIX. Este agente irá coletar informações operacionais do sistema no qual está rodando e relata os dados ao ZABBIX para processar mais adiante. Em caso de falhas (tais como HD cheio ou um processo que deixou de funcionar), o servidor ZABBIX pode imediatamente alertar o administrador que uma máquina específica reportou um erro. O agente ZABBIX é extremamente eficiente porque usa sistemas de chamadas nativo para coletar informações estatísticas. O ZABBIX pode também monitorar outros dispositivos de redes que usem um agente SNMP.

– **Interface WEB:** A fim de permitir um fácil acesso ao monitoramento dos dados e configurações através do ZABBIX, uma interface *web* é fornecida. A interface é parte do servidor ZABBIX, e é usualmente (não necessariamente) rodado em cima da máquina física e não roda no servidor ZABBIX.

3.4 - Instalação

Para instalar o ZABBIX é necessário lembrar de ter todos os requisitos de software também instalados para que não ocorra nenhum erro durante a instalação.

3.4.1 – Servidor

O primeiro passo para a instalação do servidor é a criação de um usuário no sistema operacional. Esse é o usuário que o servidor será rodado. Esta conta será criada sem alguns privilégios. Pode ser usado qualquer nome para a criação do usuário, mas o mais comum é 'zabbix'.

```
shell> adduser --system --group zabbix
```

Após isso, é preciso fazer a descompactação do arquivo '*tar.gz'* salvo do site ZABBIX antes de prosseguir a instalação. Para isso, deve ser executado o seguinte comando:

```
shell> tar -zxvf zabbix.tar.gz
```

ZABBIX vem com *scripts* SQL usados para criar o esquema de banco de dados necessário e também para inserir algumas configurações iniciais. Esses *scripts* são separados por MySQL e PostgreSQL. Para isso basta acessar o diretório onde estão os arquivos de instalação e executar os seguintes comandos:

Para MySQL:

```
shell> mysql -u -p
mysql> create database zabbix;
```

```
mysql> quit;
shell> cd create/mysql
shell> cat schema.sql | mysql -u -pzabbix
shell> cd ../data
shell> cat data.sql | mysql -u -p zabbix
```

Para PostgreSQL:

```
shell> psql -U
psql> create database zabbix;
psql> \q
shell> cd create/mysql
shell> cat schema.sql | psql -u zabbix
shell> cd ../data
shell> cat data.sql | psql -u zabbix
```

Após a criação do banco de dados, o administrador deve compilar o código fonte tanto para o servidor quanto para o agente. Para compilar o código fonte do servidor, deverá ser especificado qual o banco de dados que será usado.

```
shell> .configure --enable-server --with-mysql --with-net-snmp # Para MySQL
```

ou

```
shell> .configure --enable-server --with-pgsql --with-net-
snmp # Para PostgreSQL
```

Se for necessário distribuir binários compilados para diferentes servidores, deve ser usada a *flag --enale-static* para ligar bibliotecas estaticamente.

A *flag --with-ucd-snmp* pode ser usada em vez de *--with-net-snmp*. Se não for necessário o suporte ao SNMP, essas flags devem ser descartadas. Por fim para instalar basta executar o seguinte comando:

```
shell> make install
```

Por padrão, o comando *make install* irá instalar todos os arquivos em */usr/local/bin*, */usr/local/lib* e etc. Pode ser usado também um prefixo de instalação usando o comando *--prefix*.

Depois da instalação do código, o administrador pode incluir as seguintes linhas no arquivo */etc/services.*

```
zabbix_agent 10050/tcp
zabbix_trap 10051/tcp
```

Estas linhas não são requisitos básicos para o funcionamento. Entretanto, é recomendado a inclusão das mesmas. Se o administrador pretender usar o *zabbix_agent* em

vez do recomendado, *zabbix_agentd*, as seguintes linhas devem ser adicionadas no arquivo */etc/inetd.conf*. Para que as alterações tenham efeito, o serviço *inet* deverá ser reiniciado.

```
zabbix_agent stream tcp nowait.3600 zabbix
/opt/zabbix/bin/zabbix_agent
```

Após isso, o arquivo */etc/zabbix/zabbix_agent.conf* deve ser configurado para toda máquina que possuir o agente *zabix_agent* instalado. É neste arquivo que deve conter o endereço IP do servidor ZABBIX. Conexões para outras máquinas devem ser eliminadas. Para fazer isso o administrador poderá ver como exemplo o arquivo *misc/conf/zabbix_agent.conf*.

Outro arquivo a ser configurado em toda máquina que possuir o agente *zabix_agentd* instalado é o */etc/zabbix/zabbix_agentd.conf.* É neste arquivo que deve conter o endereço IP do servidor ZABBIX. Conexões para outras máquinas devem ser eliminadas. Para fazer isso o administrador poderá ver como exemplo o arquivo *misc/conf/zabbix_agentd.conf.*

Após as configurações necessárias para o agente, o administrador deverá fazer as configurações para o servidor no arquivo */etc/zabbix/zabbix_server.conf*.

Para uma instalação pequena (acima de 10 máquinas gerenciadas), os parâmetros padrões são suficiente. Entretanto o administrador pode alterar os parâmetros padrões para melhorar o

desempenho do ZABBIX. Para fazer isso o administrador poderá ver como exemplo o arquivo *misc/conf/zabbix_server.conf.*

Para a execução do *zabbix_server* do lado do servidor, o administrador deverá executar o seguinte comando:

```
shell> zabbix_server
```

Para a inicialização dos agentes é necessário executar o *zabbix_agentd* quando necessário. Para isto o administrador deverá executar o seguinte comando para todas máquinas que tiverem o agente instalado.

```
shell> zabbix_agentd
```

3.4.2 – Agente

Do lado cliente (agente) o processo é bem parecido com a instalação do servidor (gerente).

É necessário que o administrador crie uma conta de usuário no sistema operacional. Esse é o usuário que o agente será rodado. Esta conta será criada sem alguns privilégios. Pode ser usado qualquer nome para a criação do usuário, mas o mais comum é 'zabbix'.

```
shell> adduser --system --group zabbix
```

Após a criação do usuário, o administrador deverá fazer a configuração e compilação do código-fonte. O arquivo '.tar.gz' deve ser descompactado, como no processo de instalação do servidor e então deve ser feita a compilação apenas do agente, uma vez que não há necessidade de instalação do gerente. Para isto o administrador deverá executar o seguinte comando:

```
shell> ./configure --enable-agent
```

Se for necessário distribuir binários compilados para diferentes servidores, deverá ser usada a *flag --enale-static* para ligar bibliotecas estaticamente. Após isso para fazer a instalação do agente, o administrador deverá executar o seguinte comando:

```
shell> make
```

Depois é necessário copiar os arquivo criados dentro do diretório bin/ para */opt/zabbix/bin* ou algum outro diretório. Outros diretório comuns são */usr/local/bin* ou */usr/loca/zabbix/bin*. A configuração do arquivo */etc/service* não é um passo requerido. Entretanto, é recomendado. Para isto basta adicionar as seguintes linhas para */etc/services* das máquinas que serão agentes:

```
zabbix_agent 10050/tcp
zabbix_trap 10051/tcp
```

Se o administrador deseja usar o *zabbix_agent* em vez do recomendado, *zabbix_agentd*, as seguintes linhas devem ser adicionadas no arquivo */etc/indetd.conf*:

```
zabbix_agent stream tcp nowait.3600 zabbix
/opt/zabbix/bin/zabbix_agent
```

Vale ressaltar que as alterações feitas no arquivo */etc/inetd.conf*, só terão efeito com a reinicialização do serviço *inet*. É necessário configurar o arquivo */etc/zabbix/zabbix_agent.conf* para toda máquina que possuir o agente *zabix_agent* instalado. É neste arquivo que deve ser configurado o endereço IP do servidor ZABBIX. Conexões para outras máquinas devem ser excluídas. Para fazer isso o administrador poderá ver como exemplo o arquivo *misc/conf/zabbix_agent.conf*.

Outro arquivo que o administrador precisa configurar é o */etc/zabbix/zabbix*_agentd.conf para toda máquina que possuir o agente *zabix_agentd* instalado. É neste arquivo que deve ser configurado o endereço IP do servidor ZABBIX. Conexões para outras máquinas devem ser excluídas. Para fazer isso o administrador poderá ver como exemplo o arquivo *misc/conf/zabbix_agentd.conf.*

Por último, o administrador deve iniciar os agentes nas máquinas gerenciadas, executando o seguinte comando:

```
shell> /opt/zabbix/bin/zabbix_agentd
```

É importante ressaltar de que não há a necessidade de rodar o *zabbix_agentd* caso o administrador tenha escolhido usar o *zabbix_agent.*

3.4.3 – Interface WEB

Para configurar a interface *web*, devem ser alterados os seguintes valores no arquivo *frontends/php/include/db.inc.php*:

```
$DB_TYPE=”MYSQL”; /* Ou “POSTGRESQL” para PostgreSQL */
$DB_SERVER=”localhost”;
$DB_DATABASE=”zabbix”;
$DB_USER=””;
$DB_PWD=””;
```

Depois dessa configuração é necessário copiar os arquivos fontes PHP para um lugar onde o servidor *web* possa encontrá-los. Os diretórios mais usados são */home/zabbix/html*, */home/zabbix/public_html* ou */var/www/html/zabbix*.

Por exemplo:

```
shell> mkdir /home/zabbix/html
shell> cp – R frontends/php/* /home/zabbix/html
```

4 – Estudo de Caso

4.1 – Apresentação do Ambiente

O ambiente que tem a necessidade de ser monitorado é de grande importância para a Telefônica Empresas, pois trata-se de um projeto de unificação de aprovisionamento de serviços de redes entre todas as Tefefônicas (telefonia fixa, móvel e empresas) que há algum tempo passaram a funcionar em conjunto. Entretanto este sistema não tem uma monitoração adequada, tendo que usar simples comandos para coletar dados.

A Telefônica possuía um sistema para cada empresa, ou seja, um para a fixa, outro para a móvel e um para a empresas. Porém ela não queria acabar com esses sistemas que há tempos funciona perfeitamente. Então o projeto foi implantar um módulo (*middlware* e *workflow*) que interligasse todos outros em funcionamento e quaisquer outros que surgissem.

O ambiente proposto consiste basicamente de uma máquina de alto grau de importância que é onde está instalada a ferramenta e banco de dados. Esta máquina é chamada de *Sarcixa*. Há também um servidor, um *switch* e uma máquina de usuário para ser melhor ilustrado o uso da ferramenta.

4.2 – Configuração do ambiente

Para ver o funcionamento da ferramenta, foi necessário a criação deste ambiente na ferramenta. Este ambiente foi criado contendo três máquinas e um *switch* como falado acima. O ambiente é simples, porém pode auxiliar no entendimento da ferramenta para uma utilização em um ambiente real, seja ele qual for.

Neste ambiente podem ser monitorados dados básicos dos servidores (como HTTPD, FTP, SSH e etc), além de parâmetros de gerenciamento específico de cada máquina como memória livre, espaço em disco e etc.

Depois de ter feito toda parte de instalação, precisa ser feito a configuração do sistema para o uso na rede e gerenciamento da mesma.

O endereço para acesso é http://127.0.0.1/zabbix. Com isso aparecerá a tela de *login*, conforme Figura 4:

Figura 4: Tela de *Login*

Por padrão o usuário 'admin', vem com a senha 'admin'. Entrando com este usuário tem-se o acesso máximo ao sistema, inclusive configurações, ou seja, é recomendável a criação de um outro usuário para acesso e trocar da senha do usuário 'admin'.
Para uso adequado é necessário que o administrador faça a configuração do sistema para ter um ambiente de teste que permita obter informações de gerenciamento.

Na tela inicial tem-se a opção “Configuração”. A partir dela podem ser vistas várias outras opções. A primeira coisa a ser feita (não obrigatória, mas recomendável) é a criação de um outro usuário.

Neste caso será criado um usuário chamado 'arl' conforme Figura 5 para verificar as informações de gerenciamento.

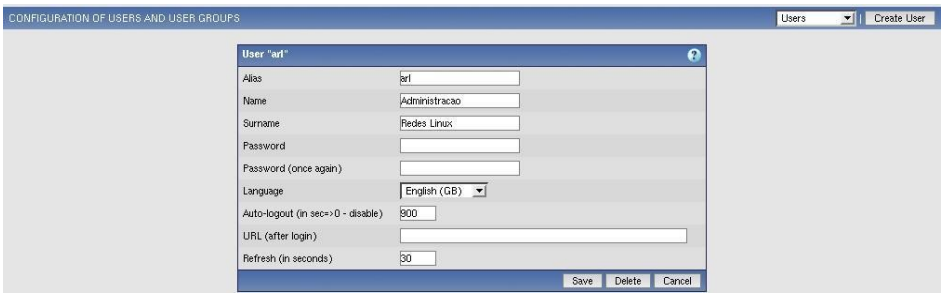


Figura 5: Cadastro de usuário

Pode ser visto nesta tela que há informações básicas dos usuários. Neste momento não há a necessidade de saber as informações sobre permissões e *e-mail* do usuário para envio de notificação.

Após a criação, o usuário aparecerá na lista de usuários. Agora para adicionar permissões ao usuário, é necessário clicar sobre o *link* '*Alias'*. Que abrirá a tela, conforme Figura 6, para a inclusão da permissão definida para o usuário.

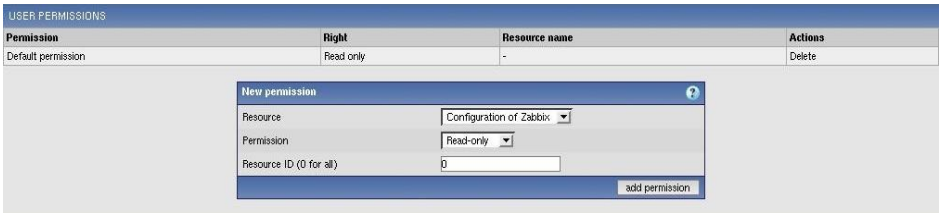


Figura 6: Atribuir permissão ao usuário

Ainda na tela de usuário, se o administrador clicar na ação '*Media'*, será aberta um tela de listas de meios de notificação, ou seja, a forma de envio de alarmes para o usuário. Para ser adicionado um meio, é necessário clicar em 'Criar' para vermos a tela conforme a Figura 7.

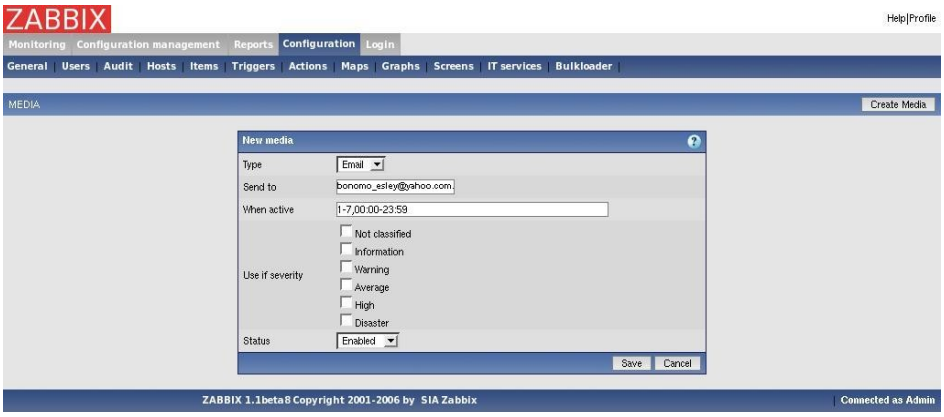


Figura 7: Criação de meios de notificação

Pode ser visto que nesta tela, além de ter das informações do *e-mail* do usuário que a notificação será enviada, há também uma outra opção muito importante, que é quando esta ação será acionada. Neste caso tem o seguinte valor:

```
1-7,00:00-23:59
```

ou seja, isso significa que sete dias da semana e vinte e quatro horas por dia, a notificação poderá ser enviada. Além disso há também o nível de severidade que esta ação irá atender. Após feito isso, o administrador deverá trocar a senha do usuário 'admin' para garantir uma melhor segurança no acesso a aplicação.

Depois de criar usuários, um outro ponto importante, não só para o ambiente de teste, é a criação de *Hosts*. No menu *Configuração --> Hosts*, aparecerá um lista de todos *as* Máquinas

Gerenciadas. Há também a opção para criar um novo *Host.* Nessa tela, há vários campos para adição de informações básicas sobre o *host* a ser adicionado, conforme Figura 8, como: o nome, grupo, se tem endereço IP ou não, a porta do agente para coleta das informações, se vai ser monitorado ou não e por último o mais importante neste momento que é qual o molde (*template*) que este *host* irá seguir. É através do molde que serão adicionados os parâmetros gerenciados sem que o usuário tenha que criar todos os parâmetros manualmente.

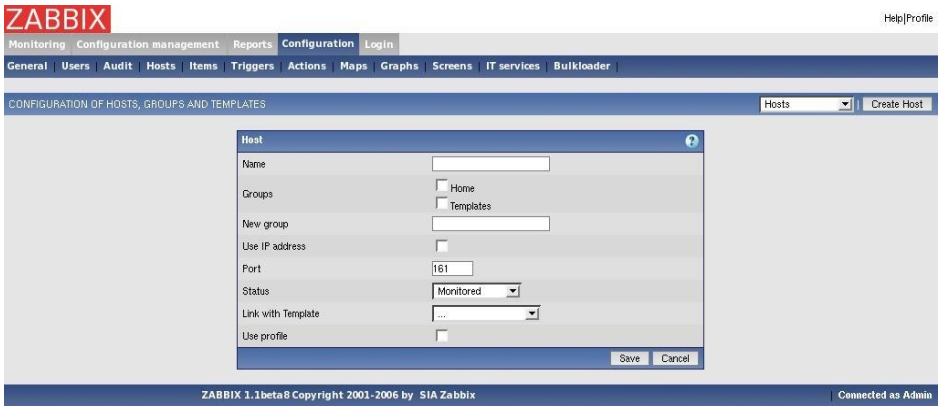


Figura 8: Cadastro de *Hosts*

Assim que o administrador terminar o cadastro do *Host,* ele aparecerá na lista de máquinas gerenciadas. Nesta tela poderá ser visualizado os Itens Gerenciados, os Gatilhos (*triggers*) e os Gráficos específicos de cada um. Os itens e gatilhos serão de acordo com o molde escolhido no cadastro.

O cadastro de máquinas gerenciadas não seria muito útil visualmente, se não fosse possível ter uma visualização da rede inteira. Então para isso existe um cadastro de mapas, onde pode ser simulado o desenho da rede, colocando os elementos (máquinas, *hubs*, servidores e etc) em uma posição específica do mapa. Além disso podem ser feitas conexões entre os elementos de rede contidos no mapa.

A criação de mapas está localizada em *Configuração* --> *Mapas*. Nesta tela é mostrado todos os mapas cadastrados e tem um botão 'Criar, o qual abrirá a tela de cadastro de mapas, conforme Figura 9.

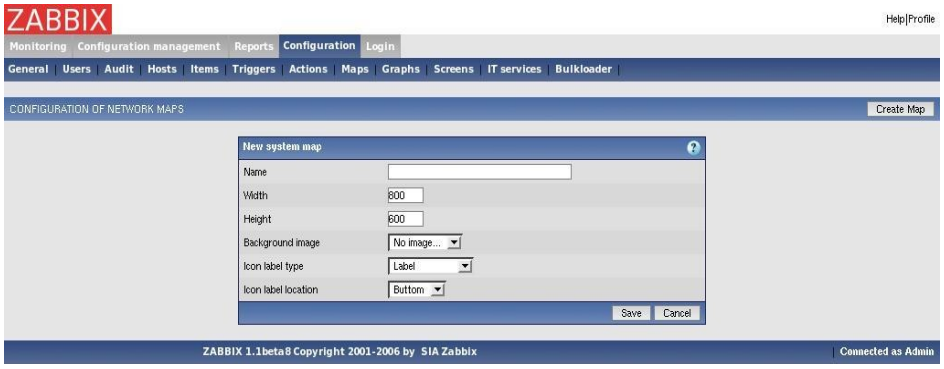


Figura 9: Cadastro de Mapa

Nesta tela pode ser observado que são informações simples de cadastro como nome, tamanho do mapa, imagem (que ainda não tem suporte na versão 1.1beta8) e posicionamento das informações do mapa. Após ser salvo, ele aparecerá na lista de mapas. E para cada mapa existe um botão de *Editar* que permitirá

a adição de máquinas no mapa. A Figura 10, mostra um cadastro de elementos na rede.

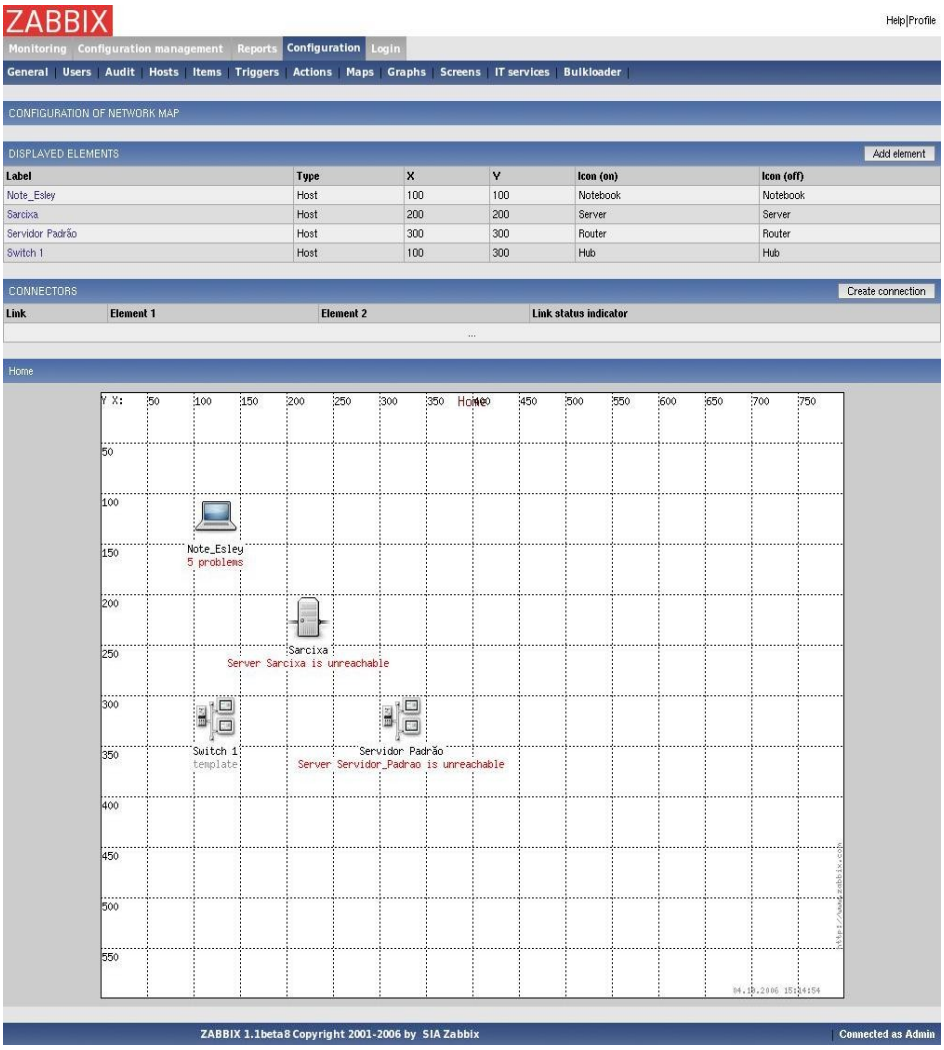


Figura 10: Elementos Cadastrados

Após ter feito o cadastro, já tem-se um ambiente básico para teste das funcionalidades e para o estudo de caso. Logicamente existem muitas funções de configurações a mais. Porém não será abordado tudo pelo simples fato de que não há a necessidade de entrar em tantos detalhes de configuração, pois o tempo e o trabalho não propõe um estudo minucioso da ferramenta. Isso poderia ficar para um estudo futuro.

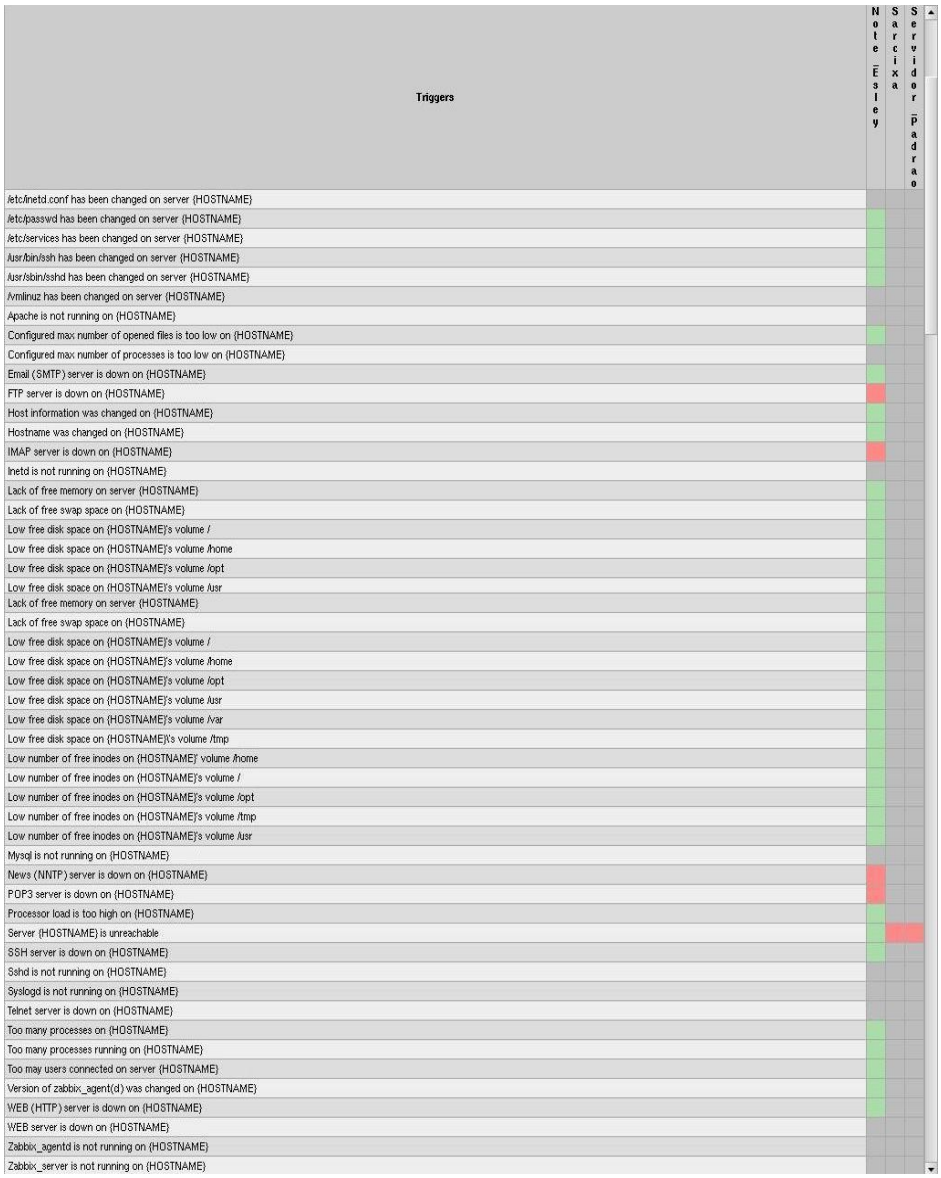
4.3 – Utilização e estudo do ambiente

Após a configuração básica de um ambiente de rede de teste, pode ser visto o comportamento e utilização dos serviços e parâmetros gerenciados para entender melhor o funcionamento da ferramenta e em que ela pode nos ajudar. Inicialmente no menu “Monitoramento” tem-se a opção de “Resumo”, que mostra a grosso modo os estados baseados nas *triggers* de alguns serviços mostrando a cor vermelho para os casos com problemas e verde os casos que estão em perfeito funcionando.

Com esta visão, pode ser identificado rapidamente como está o funcionamento dos serviços da rede, pois mostra todos os elementos gerenciáveis da rede. A Figura 11, mostra esta tela para o ambiente criado para este estudo de caso.

Pode ser percebido que as três máquinas cadastradas na nossa rede, e que foram definidas como monitoradas, estão presentes na tela de resumo. Entretanto somente uma possui

dados gerenciados reais, pois as outras não têm nem agente SNMP instalado, nem o servidor ZABBIX. As outras duas estão com o estado de “Servidor {HOST_NAME} inalcançável”, não permitindo assim a coleta das informações necessárias para o gerenciamento. Se tivesse nestas máquinas um agente SNMP, poderia ser instalado um servidor ZABBIX para coletar todas informações necessárias para a gerência. Entretanto como nestas máquinas não haviam **permissões** de instalação, não foi possível efetuar isso.



Triggers	Note_Esley	Sarcixa	Servidor_Padrao
/etc/inetd.conf has been changed on server {HOSTNAME}			
/etc/passwd has been changed on server {HOSTNAME}			
/etc/services has been changed on server {HOSTNAME}			
/usr/bin/ssh has been changed on server {HOSTNAME}			
/usr/sbin/sshd has been changed on server {HOSTNAME}			
/vmlinuz has been changed on server {HOSTNAME}			
Apache is not running on {HOSTNAME}			
Configured max number of opened files is too low on {HOSTNAME}			
Configured max number of processes is too low on {HOSTNAME}			
Email (SMTP) server is down on {HOSTNAME}			
FTP server is down on {HOSTNAME}			
Host information was changed on {HOSTNAME}			
Hostname was changed on {HOSTNAME}			
IMAP server is down on {HOSTNAME}			
Inetd is not running on {HOSTNAME}			
Lack of free memory on server {HOSTNAME}			
Lack of free swap space on {HOSTNAME}			
Low free disk space on {HOSTNAME}'s volume /			
Low free disk space on {HOSTNAME}'s volume /home			
Low free disk space on {HOSTNAME}'s volume /opt			
Low free disk space on {HOSTNAME}'s volume /usr			
Lack of free memory on server {HOSTNAME}			
Lack of free swap space on {HOSTNAME}			
Low free disk space on {HOSTNAME}'s volume /			
Low free disk space on {HOSTNAME}'s volume /home			
Low free disk space on {HOSTNAME}'s volume /opt			
Low free disk space on {HOSTNAME}'s volume /usr			
Low free disk space on {HOSTNAME}'s volume /var			
Low free disk space on {HOSTNAME}\'s volume /tmp			
Low number of free inodes on {HOSTNAME}' volume /home			
Low number of free inodes on {HOSTNAME}'s volume /			
Low number of free inodes on {HOSTNAME}'s volume /opt			
Low number of free inodes on {HOSTNAME}'s volume /tmp			
Low number of free inodes on {HOSTNAME}'s volume /usr			
Mysql is not running on {HOSTNAME}			
News (NNTP) server is down on {HOSTNAME}			
POP3 server is down on {HOSTNAME}			
Processor load is too high on {HOSTNAME}			
Server {HOSTNAME} is unreachable			
SSH server is down on {HOSTNAME}			
Sshd is not running on {HOSTNAME}			
Syslogd is not running on {HOSTNAME}			
Telnet server is down on {HOSTNAME}			
Too many processes on {HOSTNAME}			
Too many processes running on {HOSTNAME}			
Too may users connected on server {HOSTNAME}			
Version of zabbix_agent(d) was changed on {HOSTNAME}			
WEB (HTTP) server is down on {HOSTNAME}			
WEB server is down on {HOSTNAME}			
Zabbix_agentd is not running on {HOSTNAME}			
Zabbix_server is not running on {HOSTNAME}			

Figura 11: Resumo da Rede Gerenciada

Além do resumo, pode ser visto os últimos valores configurados para para os parâmetros gerenciados. O resultado é mostrado em forma de tabela contendo o nome do parâmetro, a última hora de verificação de mudança, o último valor e a mudança. Além disso tem-se a opção de verificar um Gráfico, para valores numéricos e um histórico para valores não numéricos. A Figura 12 mostra melhor esta tela.

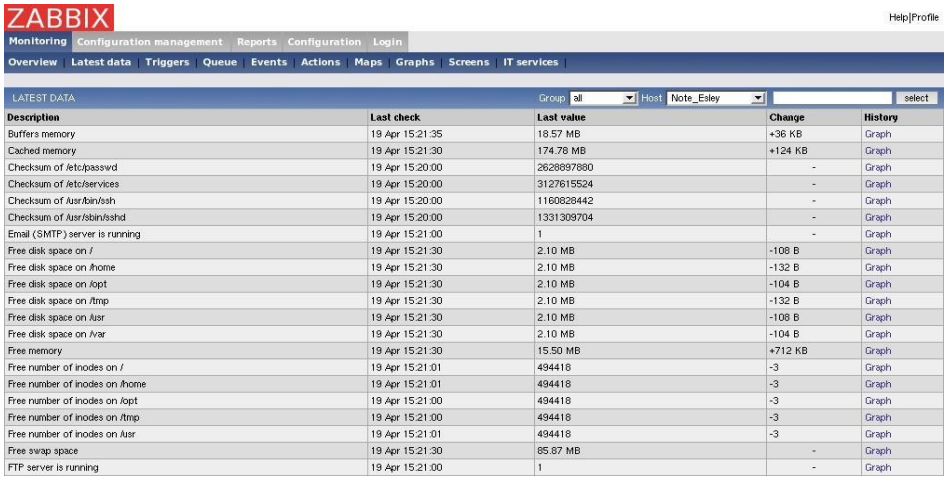


Figura 12: Últimos estados

Ao clicar no *link* Gráfico de algum parâmetro onde o valor seja numérico, abrirá uma tela com um gráfico mostrando a evolução do valor durante um determinado tempo. Dependendo do parâmetro, é através deste gráfico que pode ser feito uma análise e depois tomar decisões para solucionar problemas relacionados ao planejamento de capacidade. Por exemplo, se o parâmetro é relacionado ao uso da memória, o administrador

poderá ver se há a necessidade de colocar mais memória física. A Figura 13 mostra um exemplo do parâmetro Memória Livre para o *host* 'Note_Esley'.

Figura 13: Gráfico de Memória Livre

Para os casos de valores numéricos, em vez de um gráfico, é mostrado um histórico de mudança de valores do parâmetro desejado. A Figura14 mostra um exemplo.

Figura 14: Histórico de Itens

Além disso há as *triggers*, que nada mais são que os alarmes disparados pelos servidores notificando o administrador da ocorrência de um erro. É uma amostragem mais detalhada do que foi visto na tela de resumo. Neste ponto é tratado uma das áreas mais importantes da gerência de rede que é a Gerência de Falhas.

Nesta tela é mostrado todos os erros, os seus estados, nível de severidade, data e hora da ocorrência e dois *links*. O primeiro significa que o usuário está ciente do erro e faz o reconhecimento, como por exemplo: “Estou ciente do problema e estou tomando as medidas cabíveis” e o segundo é somente a adição de comentários.

Além das informações básicas mostrada acima, o administrador pode também mostrar mais detalhes como o parâmetro referente ao erro e as ações a serem tomadas caso essa *trigger* seja verdadeira.

Na Figura 15 pode ser visto que tem-se quatro erros para a máquinas 'Note_Esley' e um erro para cada uma das outras duas máquinas.

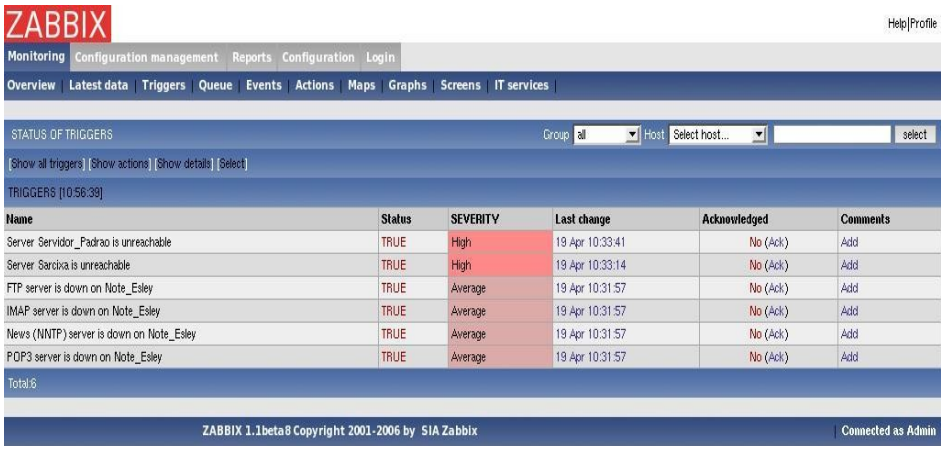
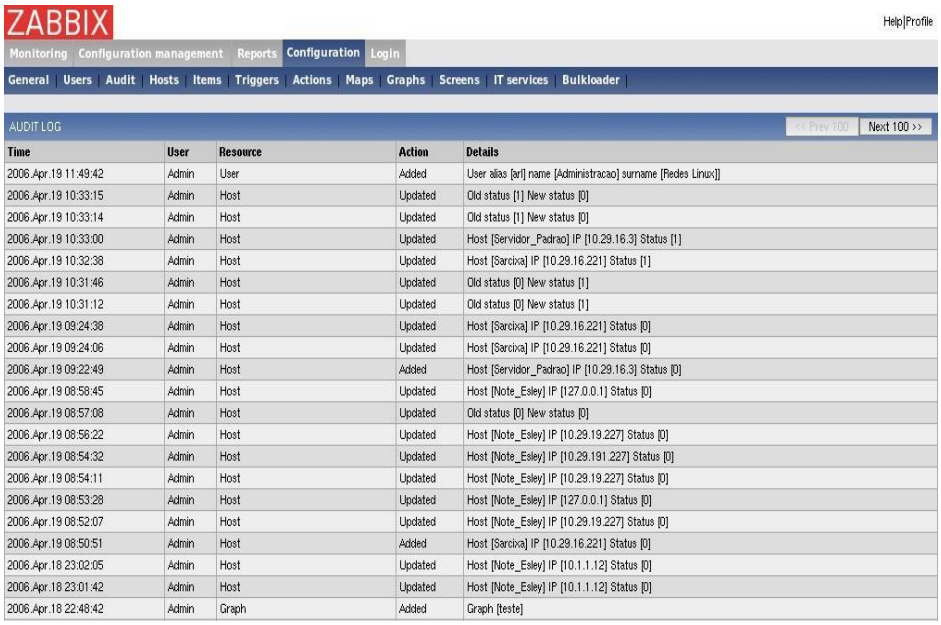


Figura 15: Estados das *Triggers*

Hoje em dia toda ferramenta que trate o mínimo que seja relacionado a segurança e controle dos dados, tem um módulo de auditoria, ou seja, um módulo que armazene toda ação feita no sistema por qualquer usuário a fim de mudar algum valor, cadastrar algum *host* e etc. A auditoria de sistemas, auxilia muito um administrador de redes a saber se alguém, e quem fez a alteração em um determinado dado. É um módulo muito poderoso na ajuda de controle das informações e segurança dos dados do sistema.



Time	User	Resource	Action	Details
2006.Apr.19 11:49:42	Admin	User	Added	User alias [arl] name [Administracao] surname [Redes Linux]]
2006.Apr.19 10:33:15	Admin	Host	Updated	Old status [1] New status [0]
2006.Apr.19 10:33:14	Admin	Host	Updated	Old status [1] New status [0]
2006.Apr.19 10:33:00	Admin	Host	Updated	Host [Servidor_Padrao] IP [10.29.16.3] Status [1]
2006.Apr.19 10:32:38	Admin	Host	Updated	Host [Sarciva] IP [10.29.16.221] Status [1]
2006.Apr.19 10:31:46	Admin	Host	Updated	Old status [0] New status [1]
2006.Apr.19 10:31:12	Admin	Host	Updated	Old status [0] New status [1]
2006.Apr.19 09:24:38	Admin	Host	Updated	Host [Sarciva] IP [10.29.16.221] Status [0]
2006.Apr.19 09:24:06	Admin	Host	Updated	Host [Sarciva] IP [10.29.16.221] Status [0]
2006.Apr.19 09:22:49	Admin	Host	Added	Host [Servidor_Padrao] IP [10.29.16.3] Status [0]
2006.Apr.19 08:58:45	Admin	Host	Updated	Host [Note_Esley] IP [127.0.0.1] Status [0]
2006.Apr.19 08:57:08	Admin	Host	Updated	Old status [0] New status [0]
2006.Apr.19 08:56:22	Admin	Host	Updated	Host [Note_Esley] IP [10.29.19.227] Status [0]
2006.Apr.19 08:54:32	Admin	Host	Updated	Host [Note_Esley] IP [10.29.191.227] Status [0]
2006.Apr.19 08:54:11	Admin	Host	Updated	Host [Note_Esley] IP [10.29.19.227] Status [0]
2006.Apr.19 08:53:28	Admin	Host	Updated	Host [Note_Esley] IP [127.0.0.1] Status [0]
2006.Apr.19 08:52:07	Admin	Host	Updated	Host [Note_Esley] IP [10.29.19.227] Status [0]
2006.Apr.19 08:50:51	Admin	Host	Added	Host [Sarciva] IP [10.29.16.221] Status [0]
2006.Apr.18 23:02:05	Admin	Host	Updated	Host [Note_Esley] IP [10.1.1.12] Status [0]
2006.Apr.18 23:01:42	Admin	Host	Updated	Host [Note_Esley] IP [10.1.1.12] Status [0]
2006.Apr.18 22:48:42	Admin	Graph	Added	Graph [teste]

Figura 16: Auditoria da Informações

Outro ponto bem interessante é a usabilidade do que foi feito na configuração, que é o cadastro de mapas. É bem interessante a possibilidade de ser ver o mapa da rede, com informações dos elementos, inclusive os erros encontrados em cada um. É uma outra forma de representar o que é visto no resumo, porém de uma maneira mais amigável.

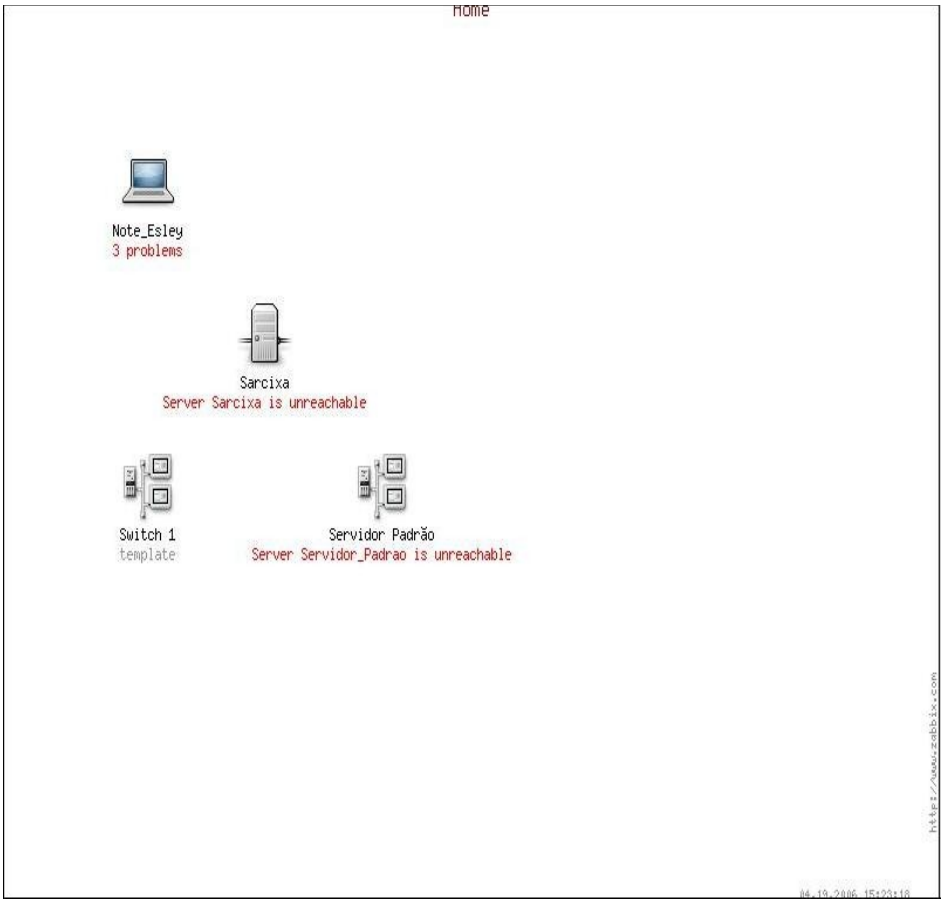
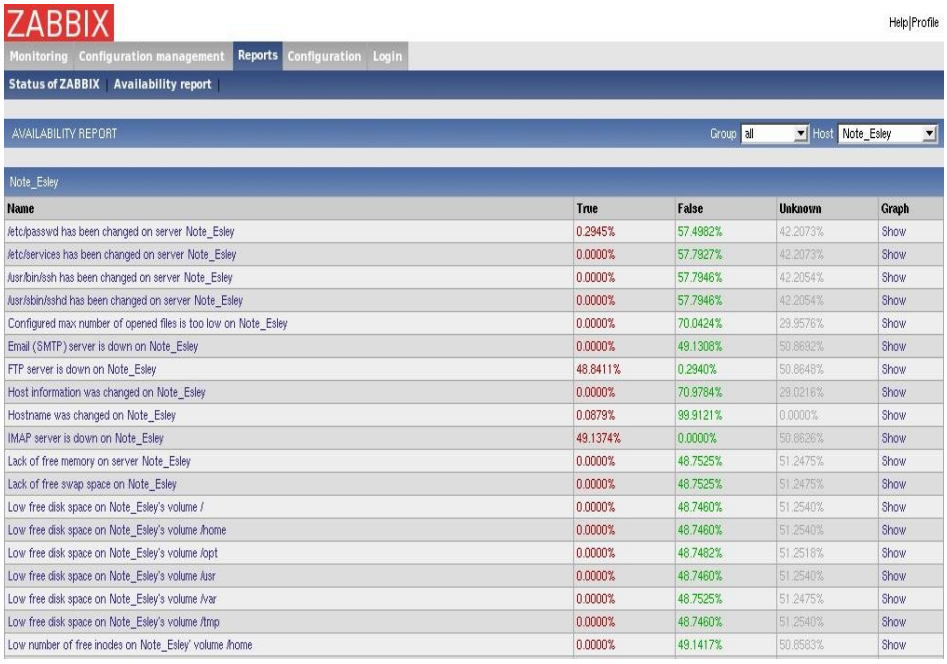


Figura 17: Mapa da Rede

Diferente de antes que havia quatro erros no *host* 'Note_Esley', agora têm-se três, e isso também é visível no mapa da rede. Foi resolvido um dos erros porque foi inicializado o serviço de FTP.

Se o elemento de rede for clicado, será mostrada a visualização dos parâmetros gerenciados.

Outra função que pode auxiliar o administrador de rede a tomar decisões para melhorar o funcionamento da rede, é a visualização de relatórios. Alguns relatórios estão disponíveis e podem ser vistos em *Relatórios --> Relatórios Disponíveis*. A Figura 18 mostra a tela de relatórios que podem ser usados.



Name	True	False	Unknown	Graph
/etc/passwd has been changed on server Note_Esley	0.2945%	57.4982%	42.2073%	Show
/etc/services has been changed on server Note_Esley	0.0000%	57.7927%	42.2073%	Show
/usr/bin/ssh has been changed on server Note_Esley	0.0000%	57.7946%	42.2054%	Show
/usr/sbin/sshd has been changed on server Note_Esley	0.0000%	57.7946%	42.2054%	Show
Configured max number of opened files is too low on Note_Esley	0.0000%	70.0424%	29.9576%	Show
Email (SMTP) server is down on Note_Esley	0.0000%	49.1308%	50.8692%	Show
FTP server is down on Note_Esley	48.8411%	0.2940%	50.8648%	Show
Host information was changed on Note_Esley	0.0000%	70.9784%	29.0216%	Show
Hostname was changed on Note_Esley	0.0879%	99.9121%	0.0000%	Show
IMAP server is down on Note_Esley	49.1374%	0.0000%	50.8626%	Show
Lack of free memory on server Note_Esley	0.0000%	48.7525%	51.2475%	Show
Lack of free swap space on Note_Esley	0.0000%	48.7525%	51.2475%	Show
Low free disk space on Note_Esley's volume /	0.0000%	48.7460%	51.2540%	Show
Low free disk space on Note_Esley's volume /home	0.0000%	48.7460%	51.2540%	Show
Low free disk space on Note_Esley's volume /opt	0.0000%	48.7482%	51.2518%	Show
Low free disk space on Note_Esley's volume /usr	0.0000%	48.7460%	51.2540%	Show
Low free disk space on Note_Esley's volume /var	0.0000%	48.7525%	51.2475%	Show
Low free disk space on Note_Esley's volume /tmp	0.0000%	48.7460%	51.2540%	Show
Low number of free inodes on Note_Esley' volume /home	0.0000%	49.1417%	50.8583%	Show

Figura 18: Relatórios disponíveis

Pode ser visto que para o serviço de FTP, quase 50% do tempo em que foi feito o gerenciamento dos *hosts* o serviço ficou parado, o que pode não ser uma boa notícia, pois pode estar acontecendo algum problema com o serviço, que não era o caso da máquina 'Note_Esley', porque o serviço realmente estava

parado. Então neste ponto, pode ser identificado a disponibilidade do serviço, ou se houve alguma mudança de estado.

Se o administrador clicar no *link Show* de algum relatório disponível, aparecerá em forma de gráficos o relatório informando a porcentagem referente a cada estado possível do item. A Figura 19 mostra um exemplo para o relatório que mostra se o arquivo */etc/passwd* foi alterado.

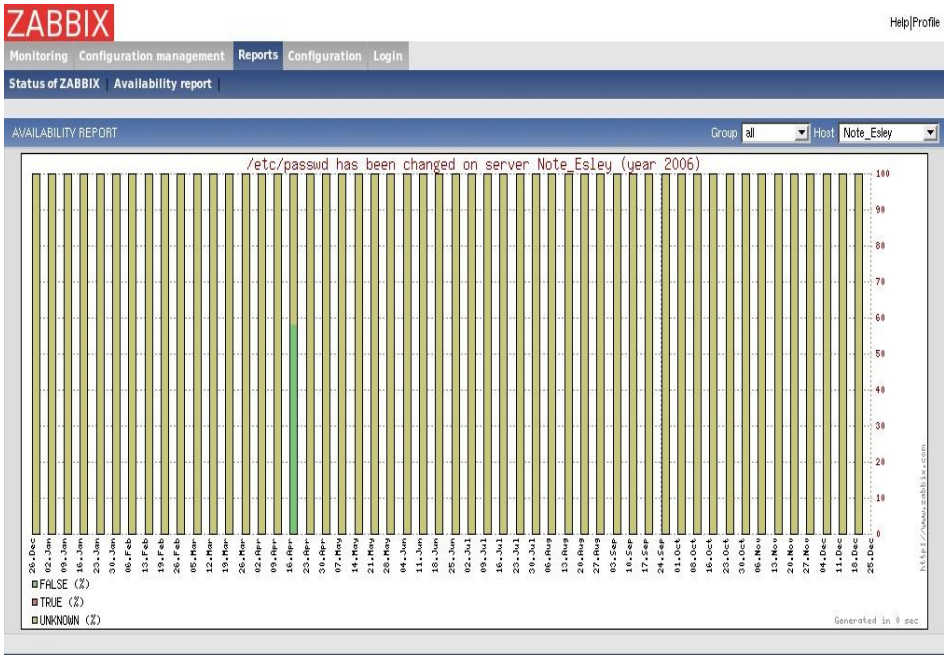


Figura 19: Relatório

Pode ser notado até aqui um caso de uso de uma ferramenta poderosa no auxílio de gerência de redes. Foi mostrado algumas funcionalidade que foram usadas na rede de

teste criada para um estudo de caso para mostrar e analisar como está o andamento da rede.

Entretanto existem muitas outras funcionalidades que não foram mostradas aqui. Mas para aprender mais sobre a ferramenta ZABBIX, é recomendável acessar o site da ferramenta. [Zab06]

5 – Conclusão

Há algum tempo, pode ser percebido que os administradores de rede têm tido diversas soluções em mãos que os auxiliem na suas tarefas de monitorar, gerenciar e garantir o bom funcionamento de suas redes. Entretanto muitas vezes não sabem qual seria a melhor solução que atenderia as suas necessidades devido às diferentes características de cada ferramenta. Todas elas tratam um único assunto que é ajudar a manter o bom funcionamento da rede, ou seja, melhorando a confiabilidade e segurança dos dados e recursos disponíveis aos usuários da mesma.

A idéia de propor um estudo sobre uma ferramenta que auxilie na gerência de rede vem da experiência com esse tipo de recurso e com a visibilidade de um grande potencial da área, seja ela usada numa rede escolar, empresarial ou qualquer outra coisa. A facilidade de entendimento e usabilidade de uma solução usando o protocolo SNMP é muito grande. A utilidade disso em qualquer rede corporativa hoje em dia é fundamental para um perfeito funcionamento da mesma.

Um outro ponto forte desta proposta é em estar trabalhando como tecnologias totalmente livres para seu uso, o que condiz muito com o propósito de quem usa o Linux, não só pela sua robustez, segurança, confiabilidade, mas também por sua liberdade.

Essa é somente uma idéia inicial, que pode crescer muito. Têm muitas áreas para serem abordadas ainda, como por exemplo, a questão de tarifação, ou seja, criação de cotas de uso aos usuários da rede através de contabilização de acesso. Outra sugestão também seria relacionada à correlação de alarmes, ou seja, um problema pode fazer com que o agente mande mais de um alarme, o que na verdade pode significar uma única coisa.

A ferramenta ZABBIX mesmo sendo um poderosíssima ferramenta, ainda é muito nova para abordar essas idéias mencionadas acima. Então espera-se que logo se tenha uma plataforma mais completa e com mais controle sobre os elementos gerenciados.

Além do ZABBIX, existem outras ferramentas que nos auxiliem em tal tarefa, como: NAGIOS, CACTI e outras. Entretanto o ZABBIX possui a facilidade de configuração e usabilidade. Além do que os gráficos são muito mais completos e com melhor desempenho em comparação com o NAGIOS.

Referências Bibliográficas

[Bri93] BRISA; **Gerenciamento de Rede, Uma Abordagem de Sistemas Abertos**. Editora Makron Books. São Paulo 1993.

[Cis99] CISCO SYSTEMS INC.: Network Management Basic, manuscrito 1999.

[Her94] HEREGEING, H-G. & ABECK, S; **Integrated Network and System Management**. Addison – Wesley. USA 1994.

[Mau01] MAURO, D.R.; SCHIMIDT, K. J. **SNMP Essencial**, Campus, 2001.

[Oda94] ODA, C. S.; **Artigo: Gerenciamento de Redes de Computadores – Noções Básicas**, 1994.

[Mon00] MONTEIRO, Eduardo Maxwell; **Metodologia para Gerência Pró-Ativa de Desempenho em Redes de Comunicação de Dados**. 2000. Tese (Mestrado) – Universidade Federal do Espírito Santo, Vitória.

[Fil06] FILHO, Huber Bernal; **Simple Network Management Protocol (SNMP)**. [on-line]. Disponível na internet via

www. url: http://www.teleco.com.br/tutoriais/tutorialsnmp/default.asp . Arquivo capturado em 21 de março 2006.

[Zab06] **ZABBIX**. [on-line]. Disponível na internet via www. url: http://www.zabbix.com. Arquivo capturado em 13 de abril de 2006.

[NSN06] **Net SNMP**. [on-line]. Disponível na internet via www. url: http://net-snmp.sourceforge.net/. Arquivo capturado em 13 de abril de 2006.

[ZNM06] **ZABBIX Network Monitoring**. [on-line]. Disponível na internet via www. url: http://www.howtoforge.com/zabbix_network_monitoring/. Arquivo capturado em 17 de abril de 2006.

[R1155] **RFC 1155 - Structure and identification of management information for TCP/IP-based internets**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc1155.html. Arquivo capturado em 23 de abril de 2006.

[R1156] **RFC 1156 - Management Information Base for network management of TCP/IP-based internets**. [on-line].

Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc1156.html. Arquivo capturado em 23 de abril de 2006.

[R1157] **RFC 1157 - Simple Network Management Protocol (SNMP)**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc1157.html. Arquivo capturado em 23 de abril de 2006.

[R1905] **RFC 1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc1905.html. Arquivo capturado em 23 de abril de 2006.

[R1906] **RFC 1906 - Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc1906.html. Arquivo capturado em 23 de abril de 2006.

[R1907] **RFC 1907 - Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)**. [on-line]. Disponível na internet via www. url:

http://www.faqs.org/rfcs/rfc1907.html. Arquivo capturado em 23 de abril de 2006.

[R2571] **RFC 2571 - An Architecture for Describing SNMP Management Frameworks**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc2571.html. Arquivo capturado em 23 de abril de 2006.

[R2572] **RFC 2572 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc2572.html. Arquivo capturado em 23 de abril de 2006.

[R2573] **RFC 2573 - SNMP Applications**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc2573.html. Arquivo capturado em 23 de abril de 2006.

[R2574] **RFC 2574 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc2574.html. Arquivo capturado em 23 de abril de 2006.

[R2575] **RFC 2575 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc2575.html. Arquivo capturado em 23 de abril de 2006.

[R1213] **RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets:MIB-II**. [on-line]. Disponível na internet via www. url: http://www.faqs.org/rfcs/rfc1213.html. Arquivo capturado em 23 de abril de 2006.

[RRDT] **Round Robin Database Tool**. [on-line]. Disponível na internet via www. url: http://oss.oetiker.ch/rrdtool/. Arquivo capturado em 25 de abril de 2006.

[MRTG] **Multi Router Traffic Grapher**. [on-line]. Disponível na internet via www. url: http://oss.oetiker.ch/mrtg/. Arquivo capturado em 25 de abril de 2006.