Monitoramento de rede com o uso do Zenoss Core

Camilo Kaneviecher[1]

[1]Instituto de Informática – Faculdade de Tecnologia Senac Pelotas
Pelotas – RS – Brasil

Resumo. *O projeto tem como objetivo, demonstrar como é realizada e utilizada de maneira simples e objetiva uma ferramenta de monitoramento de redes de computadores. Fundamental em um dia-a-dia de um Administrador de rede, por meio de ferramentas desses tipos se tem o auxilio no monitoramento e gerenciamento de sua rede, com base em relatórios e alertas administrativos podendo assim evitar futuras situações onde seja necessária sua intervenção, para uma configuração incorreta ou até mesmo para um mau funcionamento de algum dispositivo ligado a sua rede. Será apresentada a ferramenta Zenoss Core, uma ferramenta open source (gratuita), na qual foi desenvolvida com um único propósito: de auxiliar o Administrador de forma objetiva a ter um maior controle sobre sua rede.*

Abstract. *The project has the objective, demonstrate how it is made and used in a simple and objective tool for monitoring computer networks. Crucial in a day-to-day of a Network Administrator, through these types of tools you have the aid in monitoring and managing your network, based on administrative reports and alerts thus being able to avoid future situations where their intervention is needed, to an incorrect configuration or even to malfunction of any device connected to your network. Will be presented the Zenoss Core tool, an open source tool (free), in which it was developed with a single purpose: to assist the Administrator in a objective way to have more control over your network, thereby avoiding a bigger problem on your network.*

1. Introdução

Deparamos com a seguinte situação, tenho uma rede com cerca de 70 ativos, entre eles computadores, roteadores, switches etc... Nessa rede tenho serviços de e-mail e um portal web. Como fazer para gerenciar todos esses ativos e saber com antecedência, que algo está prestes a dar errado? E sendo assim evitar uma futura dor de cabeça, deixando na pior das hipóteses todos os usuários sem acesso ao e-mail ou sem acesso ao seu portal web.

Com o passar dos anos, e o crescimento significante da alta tecnologia e com a criação constante de serviços, acaba-se por impossível, um administrador de rede conseguir administrar uma rede de 70 ativos (máquina por máquina). É com isso que começou a surgir no mercado de softwares, as ferramentas de monitoramento de rede, com o intuito único de fazer o monitoramento constante de todos os ativos em sua rede.

As ferramentas de monitoramento de rede apareceram, e com elas veio a comercialização das mesmas, com valores altos e muitas vezes inviáveis para pequenas e

micro empresas que disponham de uma rede de acordo com sua infraestrutura. Com esses altos custos de software, começaram a surgir os softwares open source (código aberto), desenvolvidos por um grupo de desenvolvedores com apenas um objetivo: desenvolver softwares a mesma altura de um software pago, dando assim a oportunidade para aqueles que não tem as condições financeiras necessárias para a comercialização dos softwares pagos.

Partindo do principio do Open Source, apresentarei a ferramenta Zenoss Core, totalmente gratuita e com total suporte para mais de mil dispositivos em uma rede, de fácil implementação e configuração, voltado assim para usuários com conhecimentos básicos e dispondo de pacotes de atualização para os usuários mais avançados darem outras funcionalidades para o Zenoss de acordo com suas necessidades do dia-a-dia.

2. Zenoss Core

Zenos Core desafia o ambiente de softwares de monitoramento de rede comercial com uma solução open source (código aberto) - gratuita, onde através de uma interface web, consiga de forma intuitiva e clara, monitorar e informar sobre a situação real de seus dispositivos de rede, informando qualquer alteração, que venha ser prejudicial para sua rede, evitando possíveis falhas que poderiam lhe custar algum tempo, ou até mesmo parar todo os seus sistemas.

Zenoss Core é um aplicativo baseado em web que se instala em um servidor na rede a ser monitorada. Desenvolvido em Zope e Python, é uma ferramenta baseada em linux como a grande parte dos softwares de monitoramento encontradas no mercado.

3. Arquitetura do Sistema

A ferramenta Zenoss Core, oferece tudo que um administrador de sistema necessita para o seu dia-a-dia para descobrir, coletar, armazenar e assim podermos gerenciar nossa estrutura de TI, sem maiores complicações. O Zenoss possui uma arquitetura modular, facilitando assim a incorporação de novas funcionalidades à ferramenta. Sendo capaz de monitorar vários tipos de dispositivos.

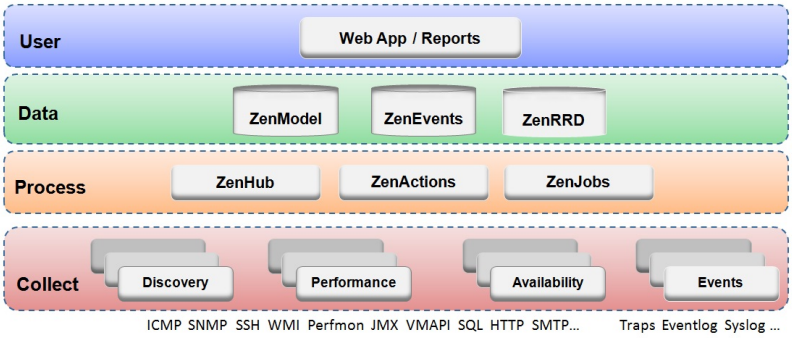

Figura 1. Arquitetura de camadas

3.1. Camada User

Zenoss é flexível o suficiente para trabalhar a partir de linha de comando, mas a maior parte do nosso trabalho será realizado através de uma interface AJAX, baseado na es-

trutura do servidor de aplicações Zope. Zope é um popular servidor de aplicação extensível escrito em Python, possui um servidor web embutido, banco de dados e modelos de HTML. Python é conhecida por ser uma linguagem de programação orientada a objetos fácil de se usar.

Através da interface web, conseguimos realizar diversas tarefas nas seguintes áreas do Zenoss:

- Navegação e Organização;
- Gerenciamento de dispositivos;
- Monitores de disponibilidade e desempenho;
- Relatórios do sistema;
- Gestão de eventos;
- Configuração e administração.

3.2. Camada de Dados

Nesta camada onde é armazenados as informações de configuração e coleta, utilizadas pelos Zenoss. Os eventos são armazenados em um banco de dados MySQL. O Zenoss gera alertas(e-mail, sinais em pager, alerta sonoro) quando um determinado limite é ultrapassado, como uma falha de servidor ou uso de memória ou CPU alta. Sendo assim determinados 3 repositórios distintos:

- ZenRRD, armazenamento de coletas temporárias e para adição de novos coletores;
- ZenModel, funcioanndo como um modelo de configuração, para dispositivos, componentes, grupos e localidades;
- ZenEvents, utilizado para armazenar dados em um banco de dados MySQL.

3.3. Camada de Processos

Conforme ao artigo [GuimarÃ£es 2010], nesta camada são geradas as comunicações entre a coleta e a camada de dados.

3.4. Camada Collect

Essa camada inclui vários serviços que reúnem informações sobre dispositivos, desempenho e eventos. Se carregam de informações retiradas de outras camadas e a distribuem em bancos de dados específicos(ZenRRD, ZenModel, ZenEvents). Utilizando nestes serviços vários daemons que dão suporte para execução da modelagem. O sistema de modelagem utiliza protocolos SNMP, SSH e WMI, para coletar informações partir das máquinas e dispositivos remotos. Após essa coleta de dados, através destes protocolos, entra em cena os plugins de modelagem que são responsável por converter os dados coletados para o formato utilizado pelo Zenoss.

4. Protocolos Utilizados

O Zenoss suporta tecnologias de monitoramento e gerenciamento, como SNMP, WMI, ping, vareduras de portas e monitoramento de portas baseado em SSH. O SNMP é o padrão para obtenção de informações e gerenciamento, sendo suportado pela grande maioria de dispositivos de rede. Para dispositivos que não dão suporte ao SNMP e nem ao WMI, é possivel realizar testes limitados, porem servindo para monitoramento baseado

em ping ou varredura de porta. O monitoramento SSH permite que o Zenoss se conecte a uma máquina e execute comandos para determinar seu estado. O Protocolo SNMP é um protocolo usado para gerenciar redes TCP/IP complexas. Também é possível usar o SNMP para monitorar o desempenho da rede, detectar problemas de rede e acompanhar quem usa a rede e como ela é usada, assim como serviços e processos.

5. Instalação e configuração do Zenoss Core

Todos os testes, de instalação e configuração foram realizados em um notebook, com 1 Gb de memória, 40 Gb de Disco Rígido e um processador Dual Core. [Zenoss 2012]Conforme a documentação do Zenoss exige uma configuração minima, mas na verdade todo caso é um caso. Para os testes o hardware disponível foi utilizado de forma satisfatória, sem perca de rendimento para 4 computares em uma rede. Uma rede até 200 máquinas se torna capaz de monitorar, obviamente conforme vai ser aplicado e dependendo da infraestrutura se exige mais da máquina, sendo assim necessário a instalação do Zenoss Core em um servidor, ou uma máquina com mais rendimento com no minimo 2 nucles. A instalação da ferramenta, acaba-se por muito simples, necessitando apenas a ter os requerimentos mínimos tanto de hardware quando de pacotes de softwares:

Deployment Size	Memory	CPU	Storage
1 to 250 devices	4GB	2 cores	1x300GB, 10K RPM drive or SSD
250 to 500 devices	8GB	4 cores	1x300GB, 10K RPM drive or SSD
500 to 1000 devices	16GB	8 cores	1x300GB, 15K RPM drive or SSD

Figura 2. Requisitos Minimos de Hardware

- MySQL 5.0.22 ou superior;
- Serviço SNMP;

A instalação resume-se em apenas algumas linhas de comando, conforme [dos Anjos Bárbara 2010]:

Instalação do MysQL e do SNMP

```
yum -y install mysql mysql-server
yum -y install net-snmp
```

Download da última versão do instalador RPM Zenoss Core, neste caso para o CentOS, no link http://www.zenoss.com/download/

Instalando o RPM Zenoss, baixado do site correspondente e encontrado no diretório que foi efetuado o download:

```
rpm -ivh zenoss-4.2.0elx86_x64.rpm
```

Logo após esse procedimento se dá inicio da instalação do pacote e dentre alguns minutos estará instalado a ferramenta Zenoss Core, antes de acessarmos uma interface web, se da inicio nos servico SNMP e o MySQL com os comandos e na propria ferramenta Zenoss Core:

```
service snmp start
service mysqld start
/etc/init.d/zenoss start
```

Iremos adicionar os serviços na inicialização do CentOS com os seguintes comandos:

```
chkconfig --level 345 mysqld on
chkdonfig --leve 345 snmpd on
```

Após esses procedimentos teremos o Zenoss devidamente instalado e pronto para ser usado, se usa um terminal qualquer, através de um navegador e coloque o ip do servidor onde se encontra o Zenoss instalado e teremos a tela de login (admin) e senha (zenoss) padrões do Zenoss Core.

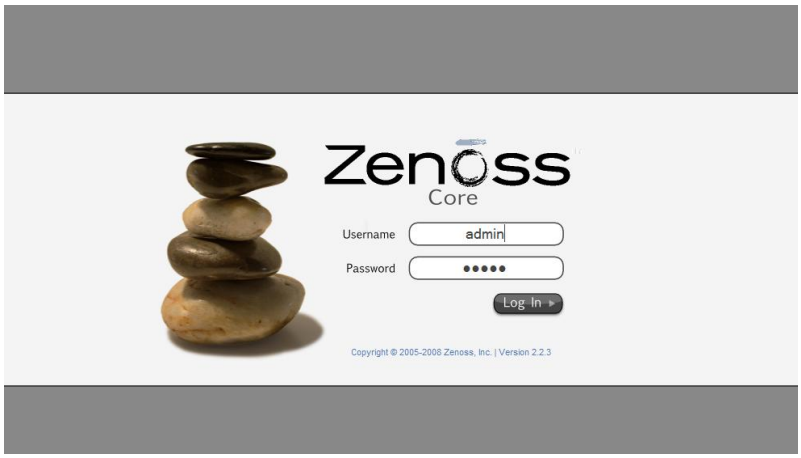

Figura 3. Tela de login

5.1. Configuração de monitoramento em máquinas Linux

Configurando o snmp.conf, conseguiremos ativar a nossa máquina linux, dando permissões para o Zenoss conseguir fazer um monitoramento completo.

Em /etc/snmp/snmpd.conf, encontre o campo Access Control Setup a SNMPv1/SNMPv2c read-only access community name e edite a linha da comunidade para public.

```
The community name to add read-only access for: public
```

Edite no mesmo snmp.conf, as seguintes linhas para que fiquem iguais as de baixo:

```
sec.name              source          community
com2sec paranoid      default         public
com2sec readonly      default         public
com2sec readwrite     default         private
```

Para meios de contatos e identificação do Administrador da rede na linha seguinte, edite conforme a sua necessidade:

```
syslocation<SETOR>syscontact<NOME DO ADM><email@dominio.com>
```

Salve esses procedimentos e entre em /etc/default/snmpd procurandoe editando a linha, no arquivo para que fique igual a de baixo:

```
SNMPDOPTS='-Lsd -Lf/dev/null -u snmp -l -smux -p/var/run/snmpd.pid'
```

Reinicie o serviço SNMP e a sua máquina ou servidor linux estará com os serviços SNMP devidamente configurados.

6. Ativando e configurando o SNMP e WMI em máquinas a serem monitoradas

6.1. Configuração de monitoramento em máquinas Windows

Com esses serviços ativos nas máquinas windows, conseguimos visualizar informações especificas das máquinas (temperatura, uso de HD, CPU, memória, programas ativos etc) e não apenas saber se estão ligadas. Verificar se instalado: services.msc, procurar na lista o item Serviço SNMP. Se não constar na lista este item, deverá ser instalado junto ao windows:

- Abra o painel de controle do Windows;
- Selecione Adicionar ou Remover componentes do Windows;
- Clique em ferramentas de gerenciamento e monitoramento e selecione detalhes
- Selecione WMI SNMP e de OK, a instalação prosseguirá, em alguns casos necessário o reinicio da máquina. Abaixo segue as imagens dos procedimentos de configuração do SNMP e do WMI, conforme figura 4 e 5 temos um exemplo.

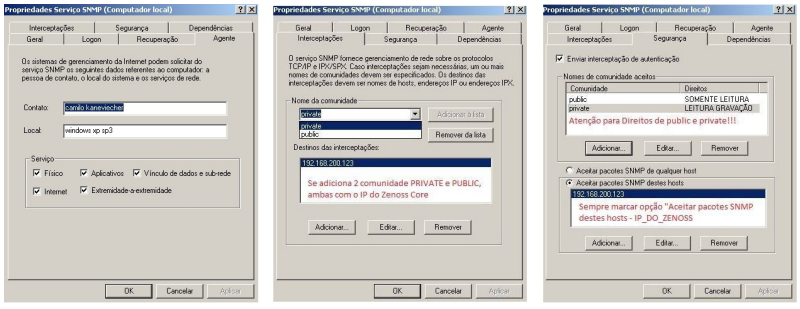

Figura 4. Configuração do SNMP no Windows

7. Funcionalidades do Zenoss Core e suas guias

Depois de instalado e feito as pré configurações já podemos acessar o Zenoss Core, através de seu navegador preferido (HTTP://IPSERVIDOR:8080), feito isso é feito o login com usuário e senha padrão do Zenoss.

7.1. A guia: DashBoard

A primeira tela acaba sendo a guia chamada DASHBOARD, onde fica localizado um resumo de toda a rede, com localização, hosts ativos, desligados. Com os logs de eventos ativos para ver a situação real de cada máquina disponível na rede, conforme figura 6.

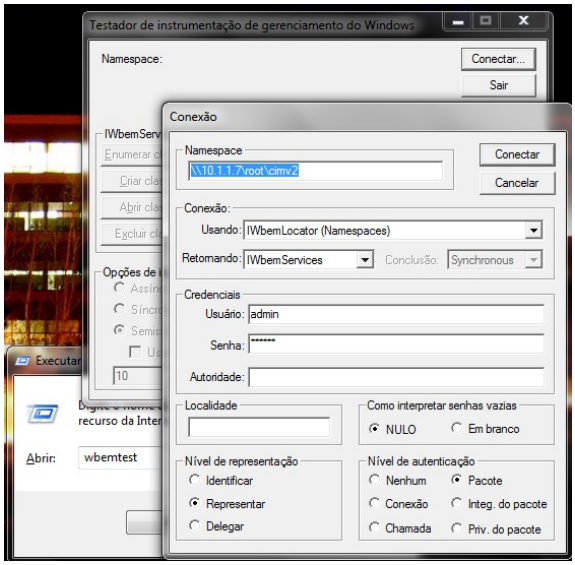

Figura 5. Configuração do WMI se necessário

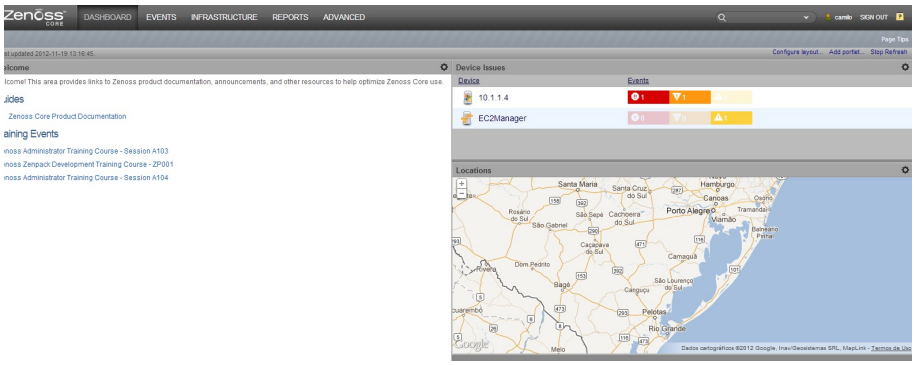

Figura 6. Tela inicial do Dash Board do Zenoss

7.2. A guia: Infra Estrutura

É onde será adicionado todos os dispositivos, lembrando que é muito importante que cada dispositivo esteja em sua devida classe, fazendo com que o Zenoss torne os dispositivos com mais opções de gerenciamento, ou seja em Servers ficarão todos os computadores, em Printers todas as impressoras e assim por diante. Temos 2 modos de adicionar os dispositivos mono device e single device

7.3. A guia: Events

Conforme [**?**] A guia events, é onde teremos todo o controle de eventos do que esta acontecendo na rede, teremos todas as notificações em todos os hosts da rede. Onde teremos avisos, para maquinas ligadas e desligadas. Assim clicando nos dispositivos teremos toda uma interface para aquele dispositivo com informações importantes para se termos o controle dos dispositivos na rede. A ferramenta vem programada para gerar alguns gráficos de performance dos dispositivos cadastrados, sendo eles de carga média no sistema, carga do processador, utilização de memória e entrada e saída.

Para acessar estes gráficos assim como a lista de hardware e software aberto de cada componente clique em Device list e escolha o dispositivo desejado para obter

informações. Logo após apenas clique na aba Perf os gráficos irão aparecer. Como mostra a figura 7.

Figura 7. Gráficos de desempenho

7.4. Guia Devices

Clicando em Devices, abre-se uma interface, onde teremos os Eventos, Dispositivos, Serviços, Processos. Nesse menu, é onde se reúne o maior numero de informações específicos de cada dispositivos, desde os processos sendo executados nas máquinas que estão sendo monitoradas, desde o hardware encontrado em cada máquina. Abaixo encontramos uma breve descrição da guia software e Hardware, onde conseguimos visualizar na guia Hardware o processador, hard disk e memórias, se a máquina possuem interfaces de expansão, também conseguimos visualiza-los. Na guia software, onde obtemos as informações de cada software instalados nos dispositivos a serem monitorados, como mostra a figura 8. Conforme o artigo [Zenoss 2012]Na guia Hardware, temos um resumo detalhado sobre o hardware dos dispositivos monitorados, como mostra a figura 9.

7.5. A guia: Reports

Fica localizado todos os logs de eventos do servidor em relação aos dispositivos conectados.

7.6. Advanced

Temos todas as configurações avançadas do Zenoss, onde por padrão já se vem configuradas, sem a necessidades de ser configuradas para o funcionamento.

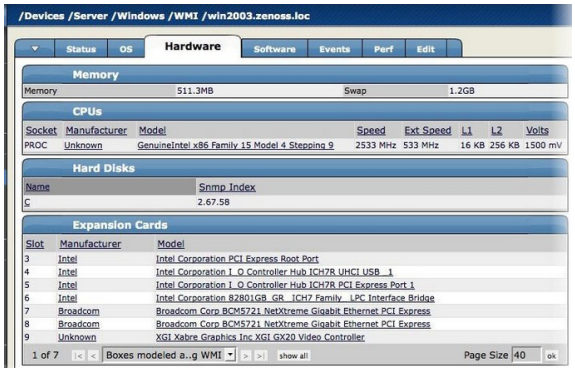

Figura 8. Lista de todo o hardware da máquina monitorada

8. ZenPacks

Conforme [Badger 2011]Zen Pack fornece uma arquitetura que nos permita personalizar o Zenoss Core, trazendo novas funcionalidades para o Zenoss. Fiz os testes com base nas interface web, no site do Zenoss Core temos vários opções de arquivos ZenPack e funcionalidades extras padrão seu Zenoss, a instalação do mesmo se ocorre de maneira pratica, onde buscamos o caminho de onde ficou o arquivo e fazemos a instalação.

Após feita a instalação é necessário o reinicio do servidor para ter efeito as modificações. Vários pacotes interessantes podem ser encontrados diretamente no site por exemplo monitores do Apache e MySQL, plugins do Cacti e Nagios também são encontrados.

9. Google Maps no Dash Board

Uma função interessante do Zenoss Core com o auxilio do Google Maps pode-se gerar mapas com as coordenadas que abrangem a área de dispersão da rede e com isso configurar e monitorar os dispositivos em suas localidades de uma forma, interativa e ilustrada, consegue-se ter com a instalação do Portlet do Google maps integrada ao Zenoss, para fornecer um status de geo-localização definido pelo usuário local de uma rede em uma cidade, estado ou pais. Por exemplo, com esse recurso pode-se verificar em tempo real, a conectividade entre sites de infra-estrutura.Conforme figura 10 e 11, temos um exemplo.

Para a configuração correta do Google Maps no zenoss core é necessário ter uma ”Google Maps API KEY”(google facilitou a vida de desenvolvedores que gostariam de criar aplicativos que tivesse a integração com o Google Maps, sem que para isso a aplicação estivesse no servidor da google. Através destas APIs, é possivel colocar o Google Maps completo em qualquer outro site, programa ou interface com suas funcionalidades do google maps.

Essa API KEY,é conseguida através do site da google (http://www.google.com/apis/maps/signup.html); Após ter a sua API KEY, basta acessar a ultima opção em SETTINGS na tela do Zenoss, onde terá o local para colocar a API KEY, salve e no dash board já aparecerá o respectivo mapa do Google Maps.

10. Alertas de e-mail

O Zenoss não seria uma ferramenta completa se não tivesse um sistema de alertas de eventuais problemas em sua rede. Se tornando uma ferramenta útil e prática com esse al-

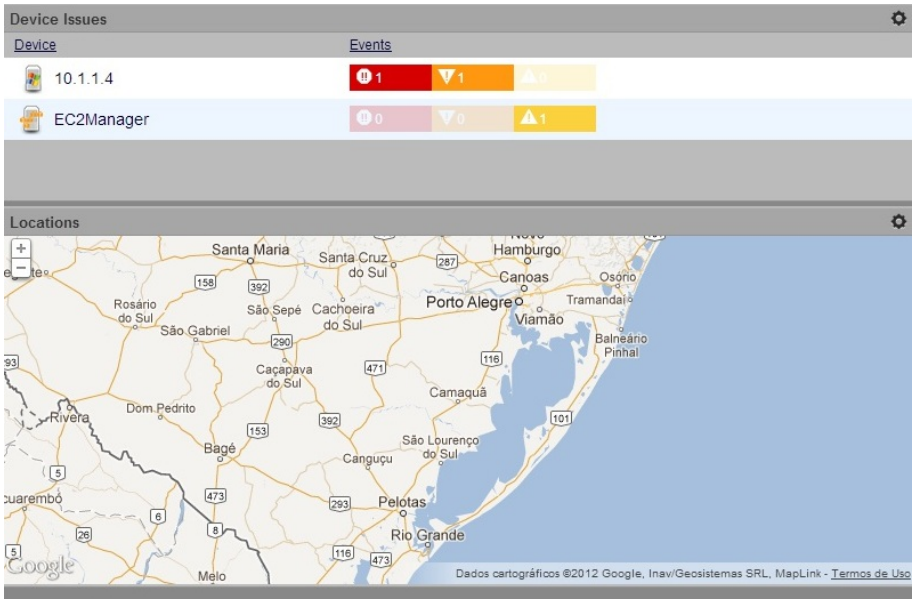

Figura 9. Tela de integração do Google Maps ao Dash Board do Zenoss com mapa do Rio Grande do Sul

ternativa de envio de alertas por e-mail, o Administrador não tem a necessidade de ficar 24 horas por dia na frente do computador monitorando a sua rede. A configuração é simples e intuitiva conforme essa imagem retirada do proprio site do Zenoss, podemos ver que a parte de configuração do mesmo, ocorre de maneira tranqüila e sem maiores complicações bastando apenas saber as configurações do seu servidor de e-mail por exemplo figura 12.

Figura 10. Exemplo com conectividade entre sites de infra-estrutura

Após feito a configuração entre em ALERTING RULES, nesse local onde criaremos as regras para o recebimento de e-ails, em severity, coloque maior ou igual a ”error”ou ”critical”. Nesse item é importante se não termos essas regras, receberemos e-mail de todos os eventos que estão ocorrendo na rede.

Figura 11. Exemplo de configuração de e-mail

11. Conclusão

Com o estudo abordado sobre a ferramenta Zenoss Core, para o monitoramento de rede, foi concluído que para um administrador de redes, ser completo em sua profissão, com certeza vai ter que se deparar com o uso dessas ferramentas de monitoramento em seu dia-a-dia. Para ter sua rede estável e sempre 100%, a melhor opção sempre vai ser o monitoramento constante, com o auxilio dessas ferramentas tornando isso muito mais pratico e fácil, com alertas enviados por e-mail e logs gerados, uma interface simples e agradável, tornando o dia-a-dia mais tranqüilo para o administrador de rede.

Podendo dessa maneira evitar, futuras dores de cabeça, quando a sua rede vier a cair sem ao menos o administrador saber o que está acontecendo. Com esse artigo, foi possível se habituar com esse ferramenta, instalada em um ambiente virtual e real, com o intuito de fazer testes e se ocorrer a oportunidade começa-la a usar em algum ambiente voltado ao meu trabalho, com a gerencia de desempenho, possíveis falhas, configuração, contabilização e segurança de um ambiente real de trabalho.

Sobre as ferramentas gratuitas ou pagas, disponíveis no mercado, cabe ao administrador e as reais condições da empresa a qual trabalha em qual escolher. Visando que as ferramentas open-source, não ficam atrás das ferramentas pagas, sempre muito completas e especificas com possíveis atualizações para outras funcionalidades. O Zenoss acaba sendo um excelente recurso de monitoramento nesse segmento open-source. Simples e eficiente, e de uma instalação e configuração fácil e rápida, tanto para usuários iniciantes quanto aos usuários mais avançados.

Referências

Badger, M. (2011). *Zenoss Core 3.x Network and System Monitoring*. PACKT puclishing.

dos Anjos Bárbara, J. V. (2010). Manual de utilização do zenoss core. *Universidade Federal de Minas Gerais*, page 11.

GuimarÃ£es, M. (2010). Monitoramento de redes com o zenoss.

Zenoss (2012). *Zenoss Core Installation*.