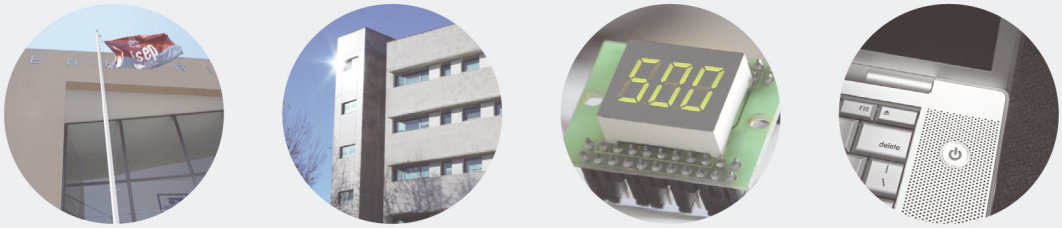
INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES



Configuração de Sistema de Monitorização

JOÃO RICARDO MARQUES CLEMENTE
Novembro de 2012

POLITÉCNICO
DO PORTO

CONFIGURAÇÃO DE SISTEMA DE MONITORIZAÇÃO

João Ricardo Marques Clemente

Mestrado em Engenharia Electrotécnica e de Computadores
Área de Especialização de Telecomunicações
Departamento de Engenharia Electrotécnica
Instituto Superior de Engenharia do Porto
2012

Este relatório satisfaz, parcialmente, os requisitos que constam da Ficha de Disciplina de Tese/Dissertação, do 2º ano, do Mestrado em Engenharia Electrotécnica e de Computadores

Candidato: João Ricardo Marques Clemente, Nº 1010180, 1010180@isep.ipp.pt
Orientação científica: Paula Marques Viana, pmv@isep.ipp.pt

Empresa:Nonius – Noniussoft S.A

Supervisão: Nelson Faria, nf@noniussoftware.com

Mestrado em Engenharia Electrotécnica e de Computadores
Área de Especialização de Telecomunicações
Departamento de Engenharia Electrotécnica
Instituto Superior de Engenharia do Porto
22 de Novembro de 2012

Poderá usar esta secção para dedicar o trabalho a alguém...

Agradecimentos

Este espaço é dedicado àqueles que deram a sua contribuição para que esta dissertação fosse realizada. A todos eles deixo aqui o meu agradecimento sincero.

Em primeiro lugar agradeço á Prof. Doutora Paula Viana a forma como orientou o meu trabalho. As notas dominantes da sua orientação foram a utilidade das suas recomendações e a cordialidade com que sempre me recebeu. Estou grato por ambas e também pela liberdade de ação que me permitiu, que foi decisiva para que este trabalho contribuísse para o meu desenvolvimento pessoal.

Em segundo lugar, agradeço ao Mestre Nelson Faria pelo constante apoio no desenvolvimento deste trabalho.

Deixo também uma palavra de agradecimento aos professores do ISEP/Academia CISCO, pela forma como lecionaram o Mestrado e por me terem transmitido o interesse por estas matérias.

Resumo

O presente trabalho enquadra-se na área das redes de computadores, fazendo referência aos protocolos e ao conjunto de equipamentos e softwares necessários para a administração, controlo e monitorização desse tipos de infra-estruturas. Para a gestão de uma rede de dados, é essencial dispor de conhecimentos e documentação de nível técnico para representar da forma mais fiel possível a configuração da rede, seguindo passo a passo a interligação entre equipamentos existentes e oferecendo assim uma visão o mais fidedigna possível das instalações.

O protocolo SNMP é utilizado em larga escala sendo praticamente um standard para a administração de redes baseadas na tecnologia TCP/IP. Este protocolo define a comunicação entre um administrador e um agente, estabelecendo o formato e o significado das mensagens trocadas entre ambos. Tem a capacidade de suportar produtos de diferentes fabricantes, permitindo ao administrador manter uma base de dados com informações relevantes da monitorização de vários equipamentos, que pode ser consultada e analisada por softwares NMS concebidos especialmente para a gestão de redes de computadores.

O trabalho apresentado nesta dissertação teve como objectivo utilizar uma ferramenta NMS, para fazer a monitorização e a gestão da infra-estrutura de comunicações de forma que permitisse conhecer em tempo real o estado dos elementos de rede, ajudar no diagnóstico de possíveis problemas, instalados pela Nonius nos diversos navios da frota Douro Azul.

O software NMS escolhido utiliza as potencialidades do protocolo SNMP para adquirir dados de monitorização de equipamentos de rede presentes na rede, bem como monitorizar redes remotas.

Abstract

The work presented in this thesis fits in the area of computer networks, more precisely in the set of protocols, equipment and software required for the administration, control and monitoring of this type of infrastructure. Efficient management of a data network, requires knowlodge and technical documentation to represent as faithfully as possible the network architecture and configuration, enabling a real view about the facilities.

The SNMP protocol is used on a large scale and is practically a standart for managing networks based on the TCP/IP technology. This protocol defines the communication between a manager and an agent, establishing the format and meaning of messages exchanged between them. It has the ability to support products from different manufacturers, allowing the administrator to maintain a database of relevant information from various monitoring equipment's, which can be viewed and analysed using an NMS software designed especially for the management of computer networks.

The work presented in this thesis aimed to use a NMS tool, to make the monitoring and management of communications infrastructure in a way that allows to know in real time the status of network elements installed by Nonius, to help diagnoses possible problems, in several ships on the fleet Douro Azul.

The NMS software chosen uses SNMP capabilities to acquire monitoring data network equipment in the network, and monitor remote networks.

Índice

Índice de Figuras

Índice de Tabelas

Acrónimos

API – Application Programming Interface

ASCII – American Standard Code for Information Interchange

ASN.1 – Abstract Syntax Notation - One

ASR – Alcatel Service Router

ATM – Asynchronous Transfer Mode

NMS – Network Manager Systems

NSCA – Nagios Service Check Acceptor

CPU – Communications Processor Unit

MIB – Management Information Base

CCTV – Closed-Circuit Television Camaras

IPTV – Internet Protocol Television

VPN – Virtual Private Network

SNMP – Simple Network Management Protocol

STB – Set-Top Box

FCAPS – Fault, Configuration, Accounting, Performance, Security

NRPE – Nagios Remote Plugin Executor

OOTB – Out-Of-The-Box

1. INTRODUÇÃO

No presente relatório, descreve-se o trabalho desenvolvido no estágio associado á unidade curricular "Tese/Dissertação", passo final para a obtenção do grau de Mestre em Engenharia Eletrotécnica e de Computadores, especialização de Telecomunicações.

O estágio decorreu em parceria com a empresa Nonius – Noniussoft S.A, e teve como objetivo o desenvolvimento de um projeto na área de gestão de equipamentos de rede, que permitisse ao candidato aplicar os seus conhecimentos de base, adquirir novas competências e que fosse de real utilidade para a empresa.

1.1. ENQUADRAMENTO

Os avanços na tecnologia de comunicação, a criação e interligação de redes de dados robustas estão a ter um efeito profundo. Para tornar isto exequível, é elementar que exista uma partilha de informação entre diversos dispositivos, estabelecendo-se assim redes de computadores que transportam dados entre si.

Em redes de computadores é habitual existirem falhas, pouco controlo, segurança que pode ser facilmente quebrada, mal funcionamento de hardware e ligações que não funcionam corretamente. Um sistema de gestão de redes com um conjunto de funcionalidades adequadas pode ajudar a controlar todos esses problemas.

Diversos modelos foram criados para possibilitar a gestão de redes, dados e telecomunicações dos quais se destacam o modelo FCAPS *(Fault, Configuration, Accounting, Performance, Security*).

Este modelo define seis áreas críticas quando se considera projetar um sistema de gestão de redes são :

1. Falhas na estrutura física - A gestão de redes ajuda a identificar falhas em ligações e colapsos em sistemas amplos de comunicação. Através da rápida identificação e isolamento dessas falhas, a resolução de problemas é facilitada.

2. Controlo - A gestão de rede permite controlar uma rede, evitando o envio de técnicos a lugares remotos e aos *Datacenters* para realizar tarefas muito simples, tais como endereçamento.

3. Mal funcionamento de hardware - Quando um router por algum motivo deixa de funcionar, o sistema todo cai. A gestão de rede pode permitir habilitar um alarme ou mesmo emitir uma notificação caso houver uma falha crítica no hardware da rede.

4. Segurança - Alguns pacotes de gestão de sistemas permitem especificar quais os serviços que podem ser acedidos e quais as máquinas podem acedê-los. Bloquear serviços é a primeira coisa a ser feita para evitar intrusos.

5. Alocação de recursos - Saber onde estão dispositivos, workstations e servidores é um aspecto importante para o gestor de uma infra-estrutura.

6. Dificuldades do utilizador final – Normalmente quando estamos a ter dificuldades em resolver certos problemas relacionados com redes, uma boa gestão de rede poderá ajudar a resolver esses problemas.

O protocolo SNMP (*Simple Network Management Protocol*), desenvolvido com o objectivo de informar o gestor de uma rede de computadores quanto ao estado em que se encontram todos os parâmetros relacionados com cada equipamento, é a solução mais adoptada.

Os sistemas NMS (*Network Management System*) que fazem a recolha de informação de forma clara e compreensível deste e outros protocolos.

1.2. APRESENTAÇÃO DO LOCAL DE ESTÁGIO

A Nonius é uma empresa tecnológica de capital 100% português, que começou por oferecer soluções de acesso à Internet para hotéis e que, desde 2009, acrescentou ao seu portfólio de produtos, uma solução de TV Interativa.

Neste momento a empresa fornece soluções e produtos para o acesso à Internet de alta velocidade para hóspedes, soluções de Televisão Interativa recorrendo a tecnologia IPTV, Sinalética Digital, Telefonia IP e Aplicações para dispositivos móveis, Internet e Televisões inteligentes.

A Nonius disponibiliza aplicações para os dispositivos móveis como Smartphones e Tablets, que permitem ao hóspede conhecer e interagir com o Hotel e os seus serviços. A aplicação Nonius Remote permite controlar a TV do quarto de Hotel e disponibilizar ao hóspede informação sobre serviços disponíveis no Hotel. Estas aplicações podem ser instaladas pelo próprio hóspede, no seu Smartphone ou Tablet, bem como serem disponibilizadas em Tablets personalizadas para o Hotel. A Nonius também desenvolve aplicações à medida da necessidade do Hotel, adaptadas à sua imagem, para iPhone e Android.

A solução de acesso à Internet da Nonius (WGServer) permite disponibilizar Internet em todo o Hotel, por Wi-Fi ou cabo. O WGServer tem funções de Gateway e Servidor para gestão de Acesso à Internet. Tem como principal aplicação a gestão e controlo de Hotspots. Combina as funcionalidades de um Hotspot Gateway e os serviços de rede um Gateway Empresarial com o Software de Gestão e Tarifação de Acesso à Internet integrado. O WGServer pode operar em modos distintos de acordo com a aplicação específica:

1. WGHotel para Hotspots Wi-Fi em Hotéis, WGBusinessPark para sistemas de controlo e distribuição de Internet em Parques Empresariais,

2. WGPublic para implementação de Hotspots Públicos e WGHotspotManager para Hotspots Distribuídos.

A linha de produtos WGServer é composta por duas plataformas de hardware diferentes, com um grau de desempenho e funcionalidades distintas, o WGS200 e o WGS5000.

Características / Equipamento	 WGS200	 WGS5000
Max Utilizadores	200	5000
Max Banda	45Mbps	750Mbps
Max VPNs	2	100
Max. VLANs	32	4096

Figura 1 WGServer – Versões do produto

A solução de TV interativa da Nonius (NiVo) disponibiliza várias opções de entretenimento e acesso a conteúdos de elevada qualidade e interesse. O hóspede tem acesso a canais de TV, aluguer de filmes, Internet, jogos, informações, promoções e compras na TV. O NiVo é um sistema multimédia interativo, de última geração, direcionado para o mercado hoteleiro e hospitalar. Esta solução IPTV oferece serviços de Video-on-Demand, canais de TV gratuitos, seleção de estações de rádio online, serviços interativos (p. ex. aluguer de bicicletas, reserva de campo de ténis, compras), serviços de informação pública (estado do tempo, farmácias de serviço, estado dos voos), acesso à Internet na TV ou por Wi-Fi, jogos, media player e serviços de localização Wireless integrado com sistemas CCTV.

O NiVo é composto por STB (*Set-top boxes*) ligadas às TVs, Backend Server responsável pela gestão e taxação de todos os serviços e pela integração com outros sistemas, IPTV Streamer cujas funções são receber e converter as emissões digitais ou analógicas de TV e rádio em formato IPTV, injetando-as na rede IP do hotel ou hospital e servidor de Video-On-Demand.

Existem três set-top boxes disponíveis na Nonius Software. A STB100 é uma set-top box Nivo que permite a visualização de TV, navegação na Internet, localização Wireless, serviços de informação, jogos, etc. Permite a conexão de um teclado/rato para uma melhor experiência de utilização.

A NiVo STB oferece, também, as funcionalidades de um Ponto de Acesso Wireless que poderá ser integrado num hotspot de hotel. A principal diferença entre a versão STB100 e a STB200 é que esta suporta resoluções HD de 1080i e 1080p. A STB80-A permite obter as mesmas funcionalidades das anteriores mas para plataformas Android, sendo este o sistema operativo do futuro para dispositivos móveis e TV.

1.3. OBJETIVOS

O objectivo principal deste projeto é fazer a monitorização dos diversos dispositivos instalados na frota Douro Azul no Porto. A Nonius, instalou soluções de televisão interativa e/ou acesso à internet, para vários navios da frota Douro Azul. Para desenvolver este projeto definiram-se um conjunto de sub-tarefas:

- Estudar ferramentas o*pensource* para monitorização de redes, e selecionar uma que satisfaça as necessidades deste trabalho;
- Efectuar testes e configurações em ambiente laboratorial testando principalmente dispositivos NiVo Backend e WGServer;
- Estudar routers com suporte de ligações VPN, pois pretende-se ter uma ligação VPN Site-to-Site entre a Nonius e a Douro Azul;
- Fazer o levantamento dos equipamentos de rede instalados nos diversos navios para serem monitorizados;
- Implementar uma solução para monitorizar dispositivos em diferentes redes;
- Proceder à devida configuração (instalar/desenvolver plugins para monitorizar um serviço específico) e validar a configuração.

2. CONCEITOS FUNDAMENTAIS E TECNOLOGIAS

No presente capítulo estão comtemplados os conceitos teóricos e o estado atual da tecnologia inerente à gestão de redes de computadores, determinantes no desenvolvimento da aplicação em análise. É feita também uma breve exposição sobre o funcionamento do protocolo SNMP, dos vários tipos de MIBs e da tecnologia VPN (*Virtual Private Network*).

2.1. SNMP – *SIMPLE NETWORK MANAGEMENT PROTOCOL*

O SNMP define um protocolo para um gestor SNMP aceder remotamente a um agente SNMP e define também que tipo de informação pode ser transferido. Foi desenvolvido para ser o mais simples possível, e é baseado em dois elementos, um gestor SNMP e um agente SNMP. A máquina servidora de gestão da rede é responsável por correr aplicações de gestão que monitorizem e controlem os dispositivos da rede. Os diversos dispositivos (routers, switchs, etc) possuem agentes que são responsáveis por realizar as funções que são requisitadas pelo gestor.

O protocolo SNMP define as regras que permitem que o gestor e os dispositivos de rede se comunicam. É um protocolo simples que permite a um administrador analisar ou alterar variáveis num dispositivo de rede a partir de uma máquina de gestão remota.

A transmissão do SNMP recorre ao UDP (*Universal Datagram Protocol)*, da família TCP/IP, para enviar informação. O UDP permite que os agentes SNMP sejam representados por um pacote simples o que faz com que o protocolo SNMP requeira um *overhead* mínimo e tenha muito pouca interferência nas outras funções da rede.

Toda a monitorização SNMP é realizada pelo sistema de gestão de rede. O gestor SNMP acede aos dispositivos de rede para obter a informação desejada ou para mudar uma variável. Nesse caso será realizada uma operação de "*polling*" (verificação do gestor). Quando os dispositivos de rede iniciam a comunicação, através do seu agente, para notificar o gestor de alterações no sistema, as suas transmissões são conhecidas como "*traps*".

2.1.1 MIBs (*MANAGEMENT INFORMATION BASES*)

A informação que um gestor SNMP pode solicitar é definida numa estrutura designada por MIB (*Manager Information Bases*) que é uma base de dados que contém definições de objetos que representam recursos efetivos que estão a ser geridos no ambiente SNMP.

Existem quatro tipos de MIBs : MIBI, MIBII, MIB experimental e MIB privada. As MIBs do tipo I e II fornecem informações gerais sobre os elementos da rede, sem levar em conta as características específicas dos equipamentos. A MIBII corresponde a uma uma evolução da MIBI, que introduziu novas informações além daquelas encontradas na MIBI tais como informações sobre operações feitas pelo protocolo SNMP. As MIBs experimentais são aquelas que estão em fase de testes, com a perspetiva de serem adicionadas à norma e que, em geral, fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos instalados. As MIBs privadas ou proprietárias foram elaboradas com o objetivo de atuar sobre um equipamento específico, possibilitando que detalhes característicos do mesmo possam ser obtidos. Desta forma, é possível obter informações sobre colisões, configuração, swap de portas, e muitas outras.

2.1.2 OPERAÇÕES DISPONÍVEIS NO PROTOCOLO SNMP

A principal característica do SNMP é a simplicidade. Ao invés de apresentar muitos comandos como outros protocolos, ele possui apenas um pequeno conjunto de operações com funções básicas de pesquisa/alteração. Através do protocolo SNMP, o cliente enviará comandos com uma de duas funções:

• Obtenção dos valores dos objetos (função GET)

• Alteração desses valores (função SET).

Está ainda previsto um mecanismo de notificação de alterações nos objetos da MIB (função TRAP). Tal estrutura torna o protocolo simples, flexível e estável, pois mantém um formato básico fixo, mesmo que novos objetos sejam implementados ou mesmo que novas operações sejam definidas, o que poderá ser feito utilizando as operações básicas.

No envio e receção de mensagens no protocolo, os nomes dos objetos não devem ser expressos na forma textual, mas sim usando uma notação numérica que representa univocamente cada um dos objectos – o OID (objecct ID).

Pode-se, resumidamente, dizer que os principais objetivos do protocolo SNMP são:

- Reduzir o custo de desenvolvimento de um agente que suporte o protocolo;
- Reduzir o tráfego de mensagens de gestão pela rede necessárias para gerir os recursos da rede;
- Reduzir o número de restrições impostas às ferramentas de gestão da rede, devido ao uso de operações complexas e pouco flexíveis;
- Apresentar operações simples, sendo facilmente usadas pelos programadores de ferramentas de gestão;
- Permitir facilmente a introdução de novas características e novos objetos não previstos inicialmene;
- Construir uma arquitetura que seja independente de detalhes relevantes à somente a algumas implementações particulares.

O protocolo SNMP define cinco operações:

- `get-request` - lê o valor dos atributos dos objetos especificados.

- `get-next-request` - obtém o nome e o valor dos atributos dos próximos objetos na ordem lexicográfica.
- `get-response` - É a resposta do agente à um pedido (request) de operação feito pelo cliente.
- `set-request` – Permite fazer a atribuição de um valor a um atributo de um objecto .
- `trap` - notificação sobre eventos ocorridos.

A operação `get-next` possibilita ao cliente descobrir qual o próximo objeto na sequência léxica assim como seu valor, introduzindo assim um mecanismo de procura de objetos na MIB. Essa operação é principalmente usada para identificar uma instância específica dentro de uma tabela de tamanho e composição desconhecida. Assim o cliente envia comandos get-next e sucessivamente obtém os nomes e valores dos atributos do objeto. Podemos assim fazer uma pesquisa na tabela sem conhecer os objetos da mesma.

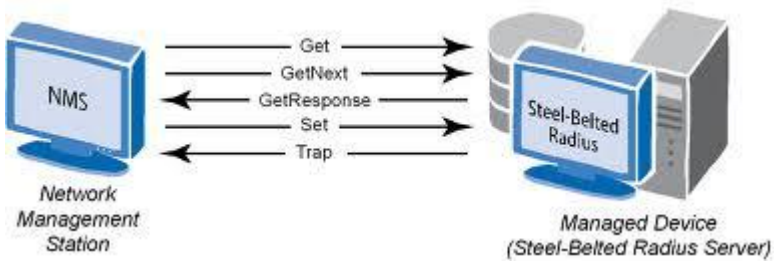


Figura 2 Exemplo de operações SNMP

2.2 VPN (*VIRTUAL PRIVATE NETWORK*)

Uma VPN é uma extensão de uma rede privada que liga dois ou mais dispositivos através de uma rede pública ou privada. Uma VPN permite o envio de informação entre dois computadores através de uma rede interna efetuando uma emulação das propriedades de uma ligação privada ponto-a-ponto. Para emular uma ligação ponto-a-ponto, a informação é encapsulada com um cabeçalho que contém as informações de routing, permitindo que a informação atravesse a rede até alcançar o extremo da ligação ponto-a-ponto. Para emular uma ligação privada, a informação enviada é encriptada. Os pacotes que são intercetados na rede são indecifráveis sem as chaves de encriptação. A parte da ligação na qual a informação é encapsulada é conhecida por túnel.

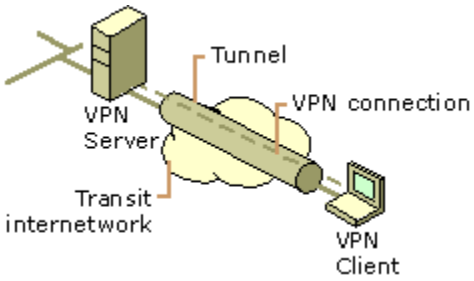


Figura 3 Ligação VPN

Uma ligação VPN permite que os utilizadores trabalhem em casa ou em qualquer local através de uma ligação segura a um servidor remoto usando uma infraestrutura fornecida por uma rede (tal como a Internet). Da perspetiva do utilizador, uma VPN é uma ligação ponto-a-ponto entre o computador de um utilizador e um servidor de uma qualquer instituição. A natureza da rede que atua como intermediário é irrelevante para o utilizador porque aparentemente a informação é enviada através de uma ligação dedicada.

2.5.1 USOS COMUNS DE VPN

As secções seguintes descrevem as configurações mais comuns de VPN.

Acesso Remoto através da Internet

A VPN fornece acesso a recursos da empresa através da rede pública (Internet) mantendo a privacidade da informação. A figura 4 ilustra uma conexão VPN usada para ligar um utilizador remoto à intranet de uma empresa.

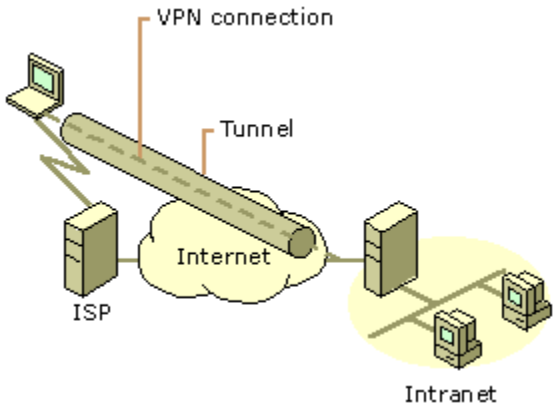


Figura 4 Utilização de uma ligação VPN para aceder a um cliente remoto numa rede privada

Usando uma ligação ao provedor de Internet local (ISP), o software VPN cria uma rede privada virtual entre o utilizador e o servidor da empresa através da rede pública (Internet).

Conexão de redes através da Internet

Existem dois métodos para a ligação de redes locais:

1. Usando linhas dedicadas para ligar uma filial à rede LAN da empresa. Em vez de usar um circuito dedicado entre a filial e a sede da empresa, ambos (a filial e sede da empresa) podem usar um circuito local dedicado e um ISP local para a ligação à Internet. O software VPN utiliza o ISP local para criar uma rede privada virtual entre a filial e a sede.

2. Usando uma linha dial-up para ligar uma filial à rede LAN da empresa. Em vez de existir um router numa filial a efetuar uma chamada de longa distância para sede da empresa, o router efetua uma chamada local ao ISP. O software VPN usa a ligação local ao ISP para criar uma rede privada virtual entre o router da filial e o router da sede da empresa através da Internet.

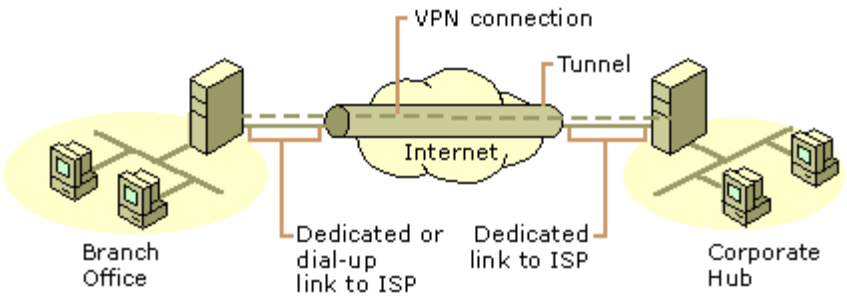


Figura 5 Utilização de uma VPN para ligar espaços geograficamente remotos

2.5.2 REQUISITOS BÁSICOS DE VPNS

Tipicamente, no desenvolvimento de uma rede, a empresa deve facilitar o acesso controlado aos recursos e às informações. Esta solução deve permitir que clientes remotos se liguem aos recursos da rede e que as filiais se liguem entre si para partilhar recursos e informações (ligações router a router). Adicionalmente a solução deve assegurar a privacidade e integridade da informação.

Para isto, uma solução VPN deve fornecer:

Autenticação de Utilizadores. A solução deve verificar a identidade do cliente VPN e restringir o acesso apenas a utilizadores autorizados. Deve também fornecer

registos de *accounting* para armazenar informação de quem acedeu, o que informação e quando.

Gestão de Endereços: a solução deve definir o endereço do cliente na intranet e assegurar que os endereços privados se mantêm privados.

Encriptação dos Dados: os dados que atravessam a rede pública devem ser ilegíveis a clientes não autorizados.

Gestão de Chaves: a solução deve gerar chaves de encriptação para os clientes e servidor.

Suporte de Multiprotocolos: a solução deve conhecer protocolos de uso comum na rede pública, incluindo IP, IPX (Internet Packet Exchange), entre outros.

O Tunneling é o método que utiliza a infraestrutura da rede para a transferência de dados através de uma outra rede. Os dados a serem transmitidos (*payload* – carga útil) podem ser pacotes de um outro protocolo. O protocolo de tunneling encapsula o pacote acrescentando um cabeçalho adicional. O cabeçalho adicional fornece informação de routing. Os pacotes encapsulados são então encaminhados entre os pontos extremos do túnel (caminho lógico) através da rede. Uma vez que os pacotes atinjam o destino, a informação é desencapsulada. O método tunneling inclui todo este processo (encapsulamento, transmissão e desencapsulamento de pacotes).

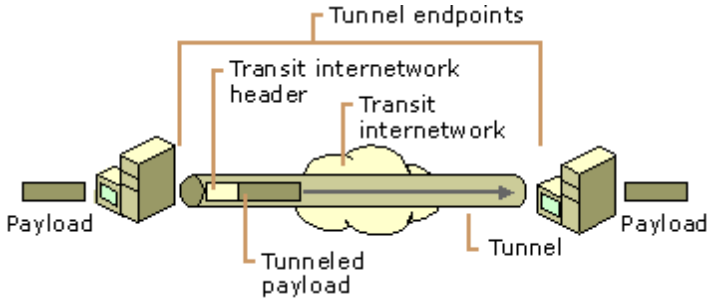


Figura 6 Exemplo de Tunneling

3. FERRAMENTAS DE MONITORIZAÇÃO DE REDES

Neste capítulo apresentam-se conceitos teóricos e práticos acerca da tecnologia inerente á gestão de redes e computadores, abordando o uso de ferramentas NMS e fazendo uma análise comparativa entre duas delas. Estas ferramentas vão permitir que os administradores de redes visualizem as informações de leitura SNMP, seja através de gráficos, tabelas, relatórios, alertas por email ou envio de sms.

3.1 ESCOLHA DAS FERRAMENTAS DE GESTÃO DE SISTEMAS

Cada organização tem prioridades diferentes em relação aos requisitos sobre monitorização de sistemas. O primeiro passo essencial quando se pretende obter soluções para monitorização de sistemas é definir quais são esses requisitos. Isto é meio caminho andado para o sucesso de um projeto. Alguns fatores de decisão na escolha da ferramenta de monitorização podem ser:

- Facilidade de utilização;
- Aptidões necessárias para implementar os requisitos vs competências disponíveis;
- Necessidade e disponibilidade de formação do utilizador;
- Custo (não só de licenças, mas do período de avaliação, manutenção e formações);
- Suporte (Relativamente ao fornecedor / fóruns);
- Escalabilidade;
- Segurança;
- Garantia (Capacidade de recorrer á equipa de suporte caso algo corra mal);

3.2 FERRAMENTAS NMS OPENSOURCE

Neste trabalho pretende-se estudar ferramentas de monitorização de redes em código aberto.

Nas secções seguintes apresenta-se duas opções de software que têm uma grande comunidade de apoio a desenvolver projectos com estas ferramentas.

3.2.1 NAGIOS

Esta ferramenta teve grande impacto a partir de 2002 num projeto chamado NetSaint. Foi desenvolvido para ser instalado em sistemas operativos Linux, e ao longo dos anos a sua instalação tornou-se cada vez mais simples.

No âmbito do projecto de tese foi utilizado, a distribuição Ubuntu Server 12.04. A configuração é possível através de uma interface disponível no url, http://localhost/nagios. O login necessário ao processo de configuração obriga à definição de um utilizador sendo o nome por omissão "nagiosadmin" e a password definida no processo de instalação. A figura x ilustra o "tactical overview" do Nagios que exibe uma visão geral dos host e serviços monitorizados.

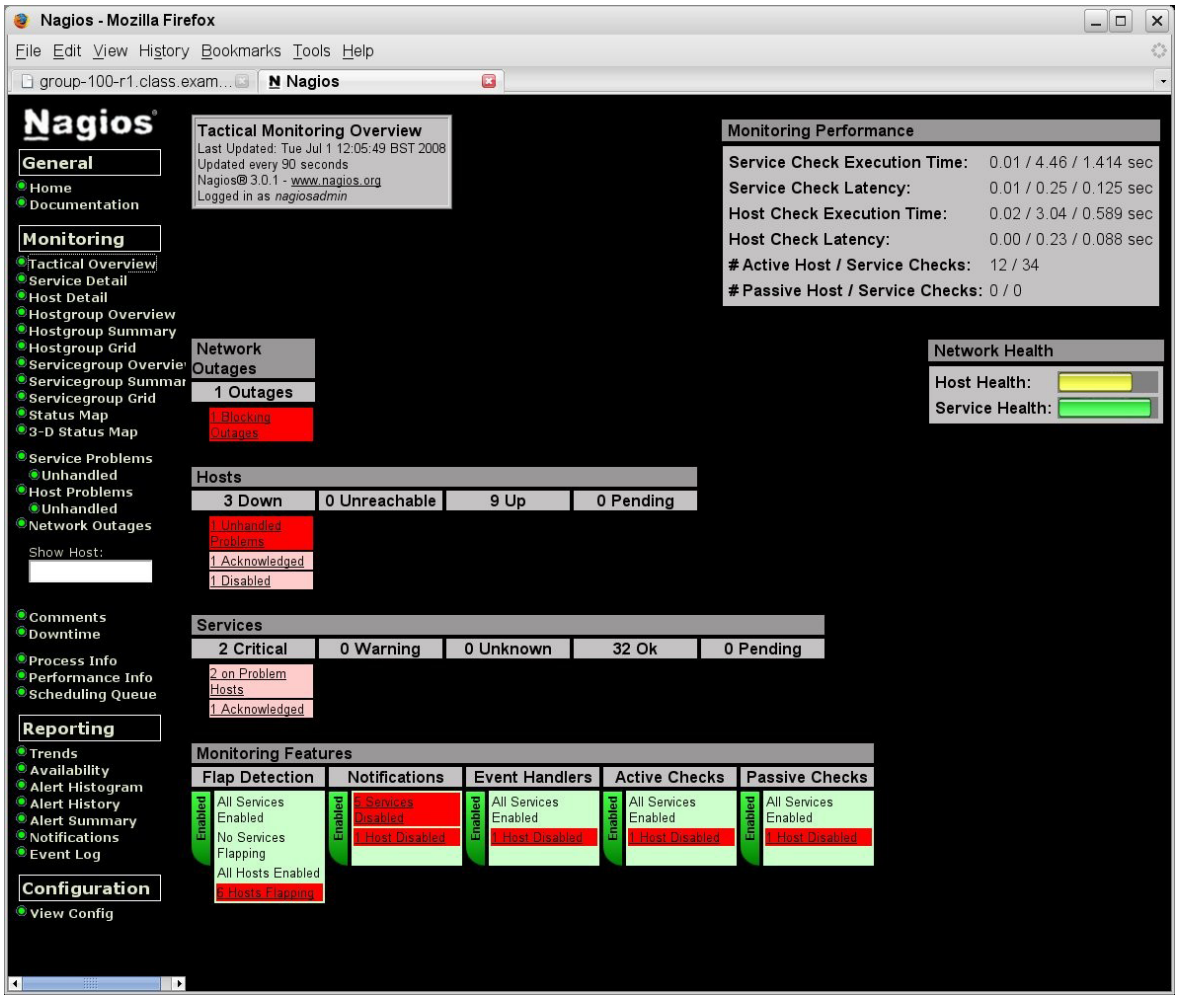


Figura 7 Visualização do Nagios Tactical Overview

3.2.2 CONFIGURAÇÃO – DESCOBERTA E TOPOLOGIA

O Nagios utiliza diversos ficheiros que definem objetos para descobrir a configuração da rede, e os seus serviços. Por omissão, existem exemplos de ficheiros de configuração disponíveis na directoria */usr/local/nagios/etc/objects*. O principal ficheiro de configuração é o *nagios.cfg* que define um largo número de parâmetros, tais como, dar permissão a utilizadores para aceder á interface do Nagios, indicar o caminho onde os ficheiros se encontram, entre outras funcionalidades.

Os ficheiros que definem os objetos são usados para definir dispositivos (*hosts.cfg*), serviços (*services.cfg*), grupos de dispositivos (*hostgroups.cfg*), contactos (*contacts.cfg*), comandos (*commands.cfg*), etc. Nestes ficheiros são definidos todos os aspetos que se pretende monitorizar e a forma de o fazer.

Conceito de objecto é utilizado para definir todos os elementos que estão envolvidos na monitorização e na lógica da notificação. Existem vários tipos de objetos:

- Services
- Service Groups
- Hosts
- Host Groups
- Contacts
- Contact Groups
- Commands
- Time Periods
- Notification Escalations
- Notification and Execution Dependencies

Os Objetos podem ser definidos em um ou vários ficheiros de configuração com a extensão *.cfg* e devemos informar no ficheiro de configuração principal nagios.cfg, deve ser indicado a directoria onde se encontram estes ficheiros.

Para monitorizar um dispositivo, é necessário definir no mínimo os seguintes objetos,

- Services
- Hosts
- Host Groups
- Contacts

Para simplificar a configuração, definiu-se um ficheiro para cada objeto e cada objecto tem as suas directivas mínimas que têm que ser especificadas.

Será apresentado a seguir exemplos de ficheiros de configuração desses objectos,

```
# Define um grupo para dispositivos de teste na Nonius

define hostgroup{

hostgroup_name  Nonius;
alias           Nonius Lab;
members         BACKENDTEST147,BACKENDTEST148,WGServerJMC;

}


# Definir um host para o BackendTEST147

define host{

host_name                BACKENDTEST147;
hostgroups               Nonius;
alias                    NiVoBackend TEST 147;
address                  10.0.0.147;
check_command            check-host-alive;
check_interval           5;
retry_interval           1;
max_check_attempts       5;
check_period             24x7;
contact_groups           admins;
notification_interval    30;
notification_period      24x7;
notification_options     d,u,r;

}
```

```
# Define o serviço "ping" para o BACKENDTEST147

define service{

host_name                   BACKENDTEST147;
service_description         PING;
check_command               check_ping!200.0,20%!600.0,60%;
max check attempts          5;
check_interval              5;
retry_interval              1;
check_period                24x7;
notification_interval       30;
notification period         24x7;
contacts                    nagiosadmin;
contact_groups              admins;
notifications_enabled       1;

}
```

Agora teremos que editar o ficheiro contacts.cfg para sermos notificados cajo haja algum alerta.

```
define contact{

contact_name                        nagiosadmin;
use                                 generic-contact
alias                               Nagios Admin;
host_notifications_enabled          1;
service_notifications_enabled       1;
host_notification_period            24x7;
service notification period         24x7;
host_notification_options           d,u,r;
service_notification_options        w,u,c,r;
host_notification_commands          notify-host-by-email;
service_notification_commands       notify-service-by-email
email                               jmc@noniussoftware.com ;

}
```

Sempre que for feita alguma alteração aos ficheiros de configuração deve ser executado o seguinte comando: */etc/init.d/nagios restart*. Existe também um comando para verificar se os ficheiros estão consistentes com as devidas regras, */usr/local/nagios/bin/nagios v/usr/local/nagios/etc/nagios.cfg*. Existe a necessidade de criar estes ficheiros para que a ferramenta descubra os dispositivos de rede.

3.2.3 CAPACIDADE DE MONITORIZAÇÃO

A capacidade de monitorização do Nagios foca-se principalmente nos sistemas em vez da rede. Tem um enorme número de plugins oficiais para monitorização, também existem comunidades a desenvolver plugins e o próprio utilizador pode desenvolver os seus.

Os plugins são instalados na directória /usr/local/nagios/libexec. O Nagios tem dois conceitos separados, monitorização de dispositivos e monitorização de serviços e existe uma relação conhecida entre o estado do dispositivo e o estado dos seus serviços.

3.2.4 GESTÃO DE EVENTOS

Nesta ferramenta a gestão de eventos está relacionada com serviços ou elementos de rede e é determinada por duas componentes:

• O estado de um serviço ou dispositivo (OK, WARNING,UP,DOWN, etc.);

• O tipo de estado do serviço ou dispositivo;

Existem dois tipos de estados no Nagios, estado SOFT e HARD. Estes estados são cruciais na logica de monitorização, sendo estes que vão determinar quando deve executar eventos e notificações. Normalmente os estados SOFT ocorrem em situações do tipo:

- Quando a validação de um serviço/dispositivo resulta num estado não-OK ou não-UP e a validação não foi executada o numero de vezes definida pela diretiva *max_check_attemps*;

- Quando um serviço/dispositivo recupera de um erro SOFT;

Enquanto que os estados HARD ocorrem por exemplo:

- Quando um dispositivo/serviço transita de um estado para o outro estado (WARNING para CRITICAL);

- Quando a validação de um dispositivo/serviço resulta de estado não-OK e corresponde ao dispositivo estar DOWN ou UNREACHABLE;

3.2.5 CONSOLA DE EVENTOS

Podemos visualizar todos os eventos, selecionando Event log no menu do lado esquerdo na interface do Nagios.

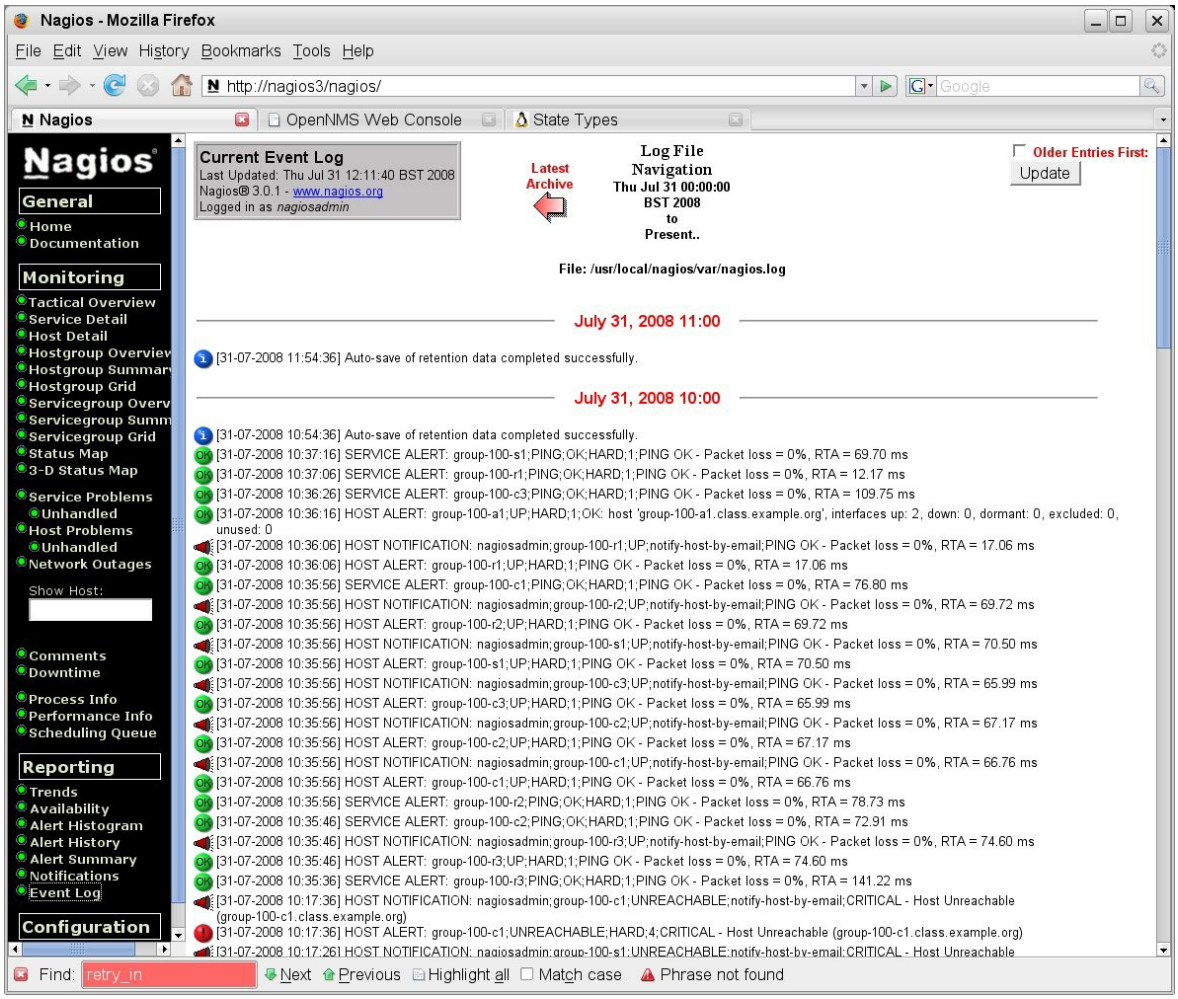


Figura 8 Log de enventos do Nagios

O log mostra o estado dos eventos e se alguma notificação foi gerada, podemos também visualizar os logs no ficheiro */usr/local/nagios/var/nagios.log*.

Em baixo do menu "*Reporting"* no lado esquerdo, tem uma opção para mostrar a informação nos eventos (Alertas). O "*Alert History"* é efetivamente o mesmo que o log de eventos, agora o "*Alert Histogram"* produz gráficos quer para os dispositivos, quer para os serviços que nos dá a possibilidade de configurar vários parâmetros para esses gráficos.

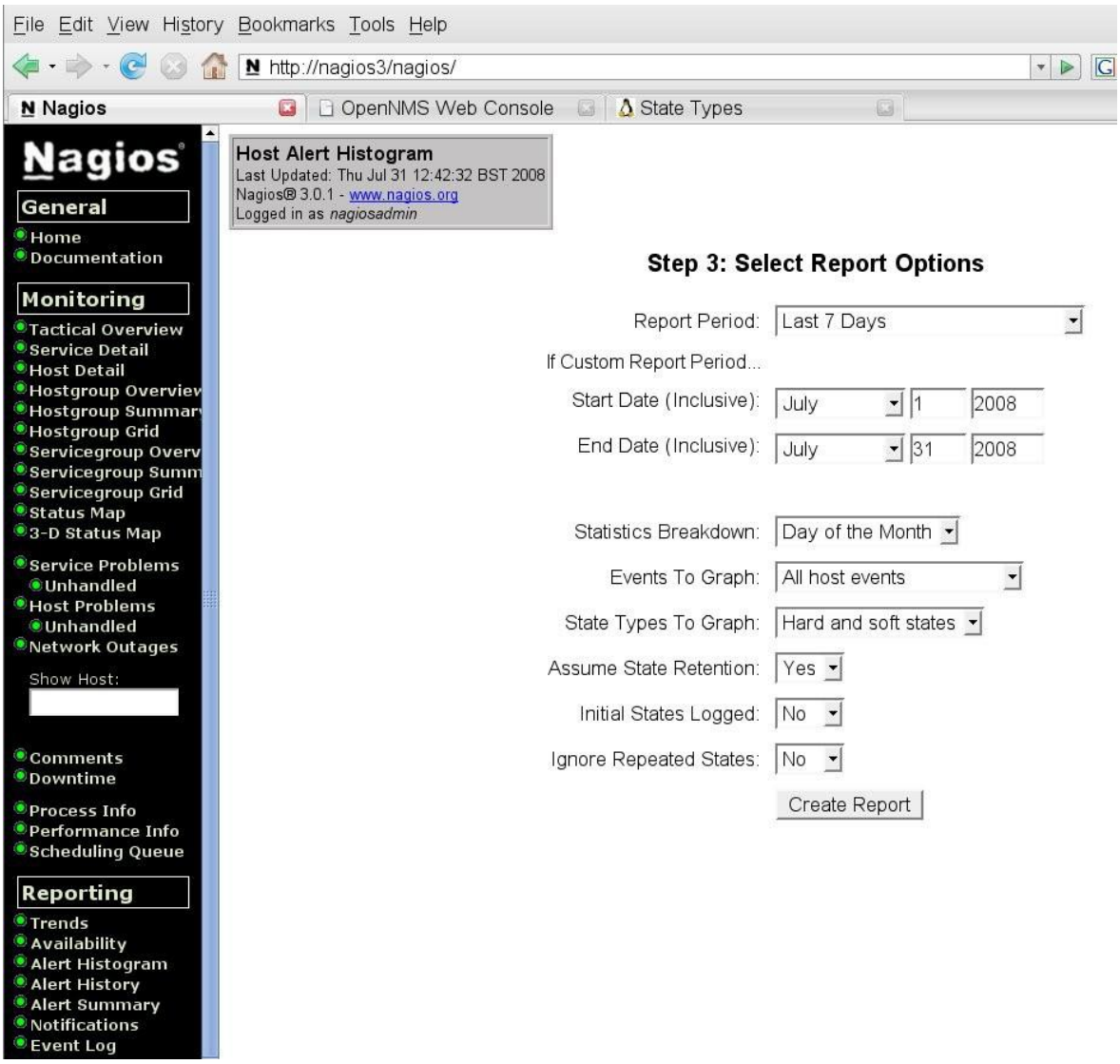


Figura 9 Configuração dos parâmetros para alertas de histogramas no Nagios

A figura seguinte mostra o resultado dos parâmetros especificados

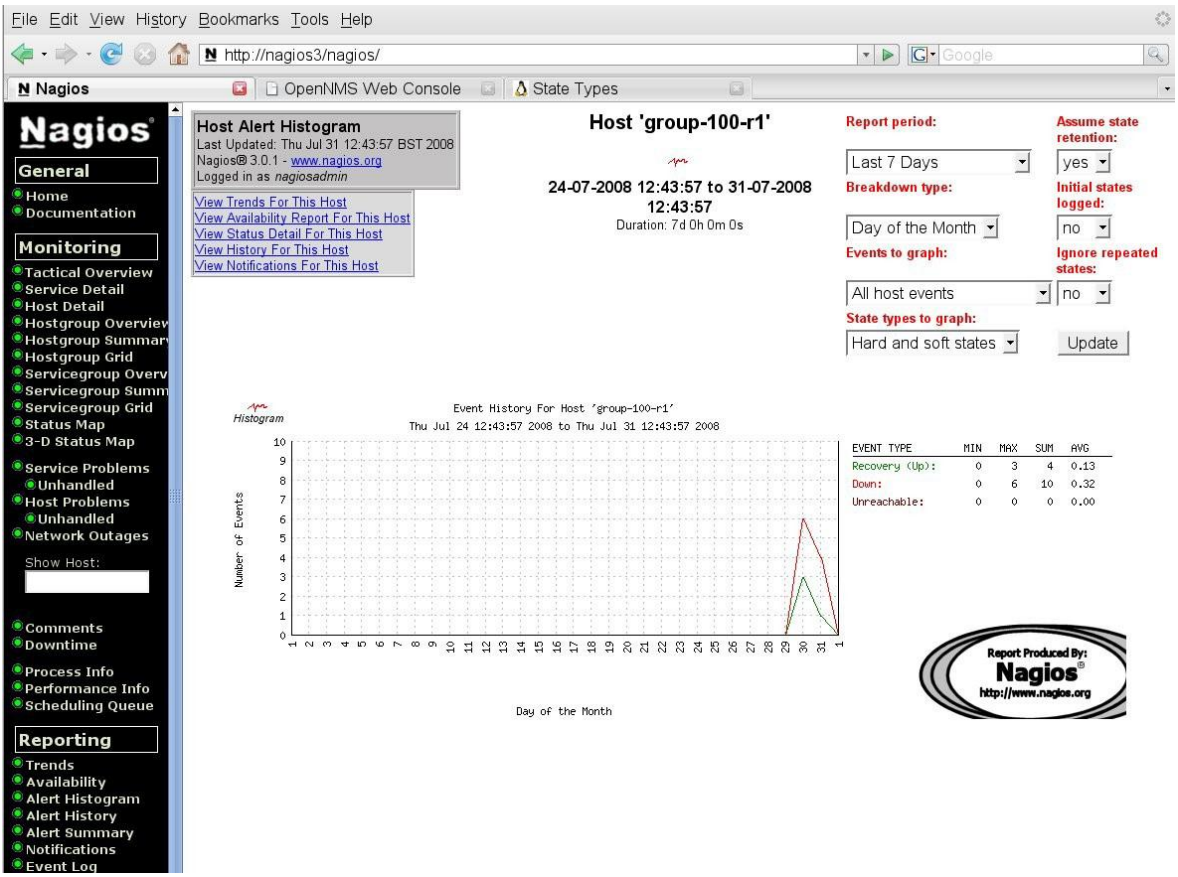


Figura 10 Alerta de histograma para o host group-100-r1

3.2.6 NOTIFICAÇÕES

Para ser possível receber notificações, é necessário editar o ficheiro *contacts.cfg* e adicionar o nosso contacto conforme as diretivas exigidas pelo Nagios. Posto isto, podemos receber notificações quando um dispositivo/serviço tem algum problema, para tal basta adicionar aos ficheiros *hosts.cfg* ou *services.cfg* as diretivas obrigatórias para tal.

3.2.7 RESUMO

O Nagios é uma ferramenta de gestão de sistemas já com alguns amos, com a melhor documentação relativamente aos softwares de código aberto. O seu forte é na validação da disponibilidade dos dispositivos e serviços. Agora no que respeita á gestão da rede não é assim tão forte, não tem descoberta automática. Todo o processo de monitorização é realizado pelos plugins que são instalados por omissão, outros estão disponíveis através de vários grupos de colaboradores, mas o próprio utilizador pode desenvolver o seu.

Um dos plugins padrão é o *check_snmp* que pode ser usado para consultar um dispositivo através de uma variável *SNMP MIB*. Logicamente essa máquina tem que ter suporte SNMP e a MIB em questão. É também possível correr validações em máquina remotas, se for instalado um agente NRPE (disponível apenas para máquinas Unix/Linux) e os plugins do Nagios no sistema remoto. Se quisermos imensos gráficos de performance então o Nagios não é a melhor opção.

O Nagios parece ser bom para a monitorização de sistemas relativamente pequenos, mas se o utilizador necessitar de um relatório com um historial de performance elaborado não é a melhor opção.

3.3 ZENOSS

A outra ferramenta de monitorização foi o Zenoss. Relativamente a este software existem duas ofertas, uma *opensource*, Zenoss Core e outra é o Zen Enterprise que vem com vários contratos de suporte e com um nível de configurações mais elaborado. Tal como o Nagios existem plugins ou extensões do Zenoss com o nome de ZenPacks, neste momento existem mais de cem plugins disponíveis. Tipicamente, os ZenPacks adicionam a habilidade de monitorizar novos tipos de dispositivos, mas também serve para adicionar novas funcionalidades no software.

O Zenoss consegue descobrir novos dispositivos automaticamente, faz a gestão de eventos e de performance. Foi desenvolvido para ambientes Linux, MAC OS X e Solaris, é web-based que é baseado no servidor de aplicações *Zope* escrito em *Pyton*. Para aceder via Web, basta indicar o url http://zenoss:8080 e especificar o username – admin e a password definida na instalação.

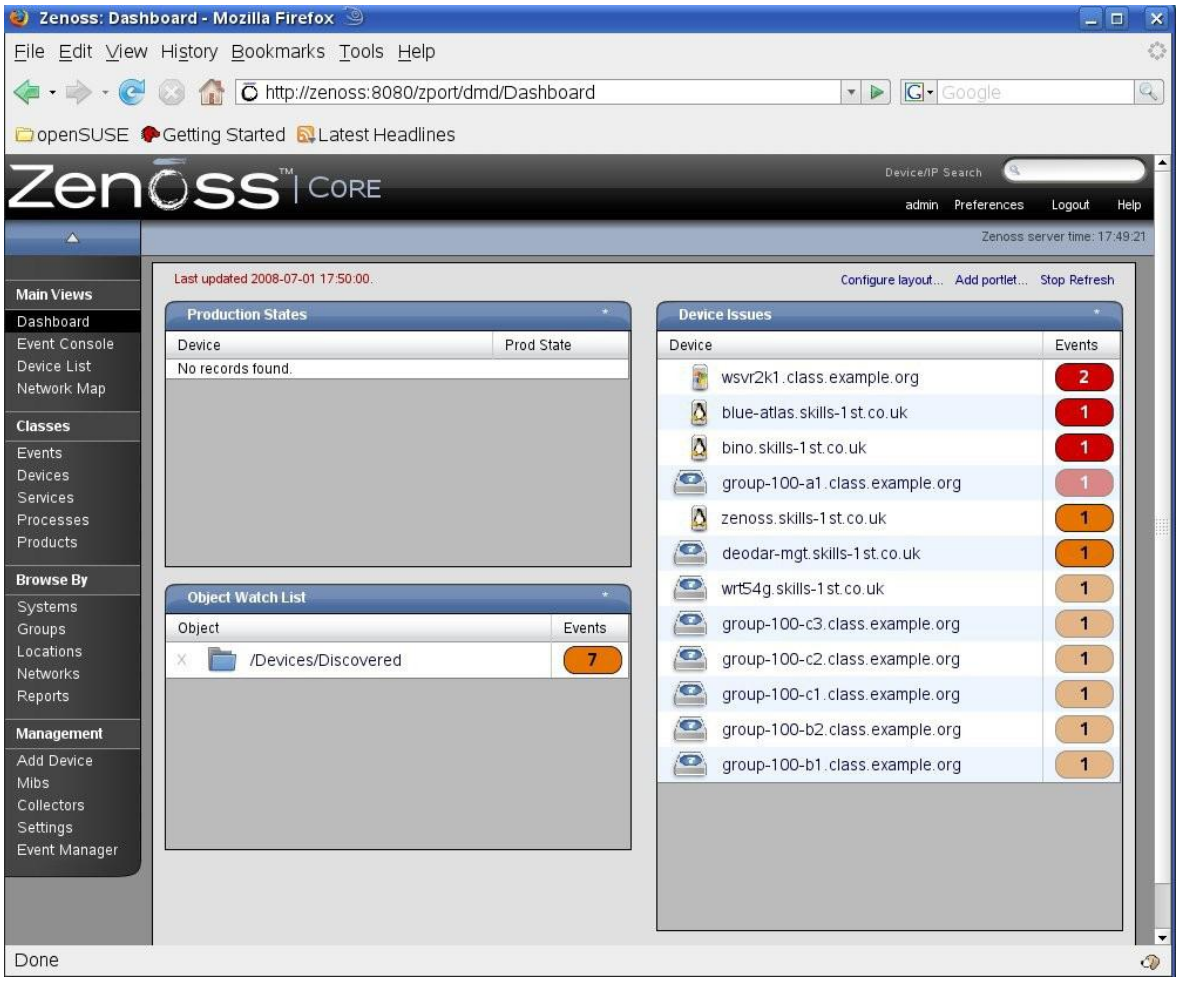


Figura 11 Dashboard do Zenoss

3.3.1 INSTALAÇÃO DO ZENOSS 3.X

A instalação foi efetuada usando o Ubuntu Server 12.04 sendo esta mais fácil que a do Nagios. Em primeiro lugar é necessário adicionar o repositório do zenoss editando o ficheiro em /etc/apt/sources.list e adicionar as seguintes linhas:

```
# Zenoss repository
deb http://dev.zenoss.org/deb main stable
```

Introduzir os seguintes comandos:

```
apt-get update
apt-cache search zenoss-stack
```

Deverá aparecer:

```
zenoss-stack - Zenoss Stack with all requirements.
```

Introduzir o comando para instalar o Zenoss stack:

```
apt-get install zenoss-stack
```

O Zenoss é instalado na diretória /usr/local/zenoss .

Por fim iniciar o Zenoss com o comando:

```
# /etc/init.d/zenoss-stack start
```

3.3.2 CONFIGURAÇÃO - DESCOBERTA DE DISPOSITIVOS

Ao iniciar o Zenoss pela primeira vez através do url http://zenoss:8080, vamos ter a possibilidade de adicionar utilizadores, definir a password para o administrador e adicionar dispositivos. Existem duas maneiras para adicionar dispositivos, uma manual, em que indicamos a rede (por ex : 10.0.0.0/24) ou um intervalo na rede (por ex: 10.0.0.50 – 250) e outra automática em que basta selecionar a opção *Autodiscover devices*.

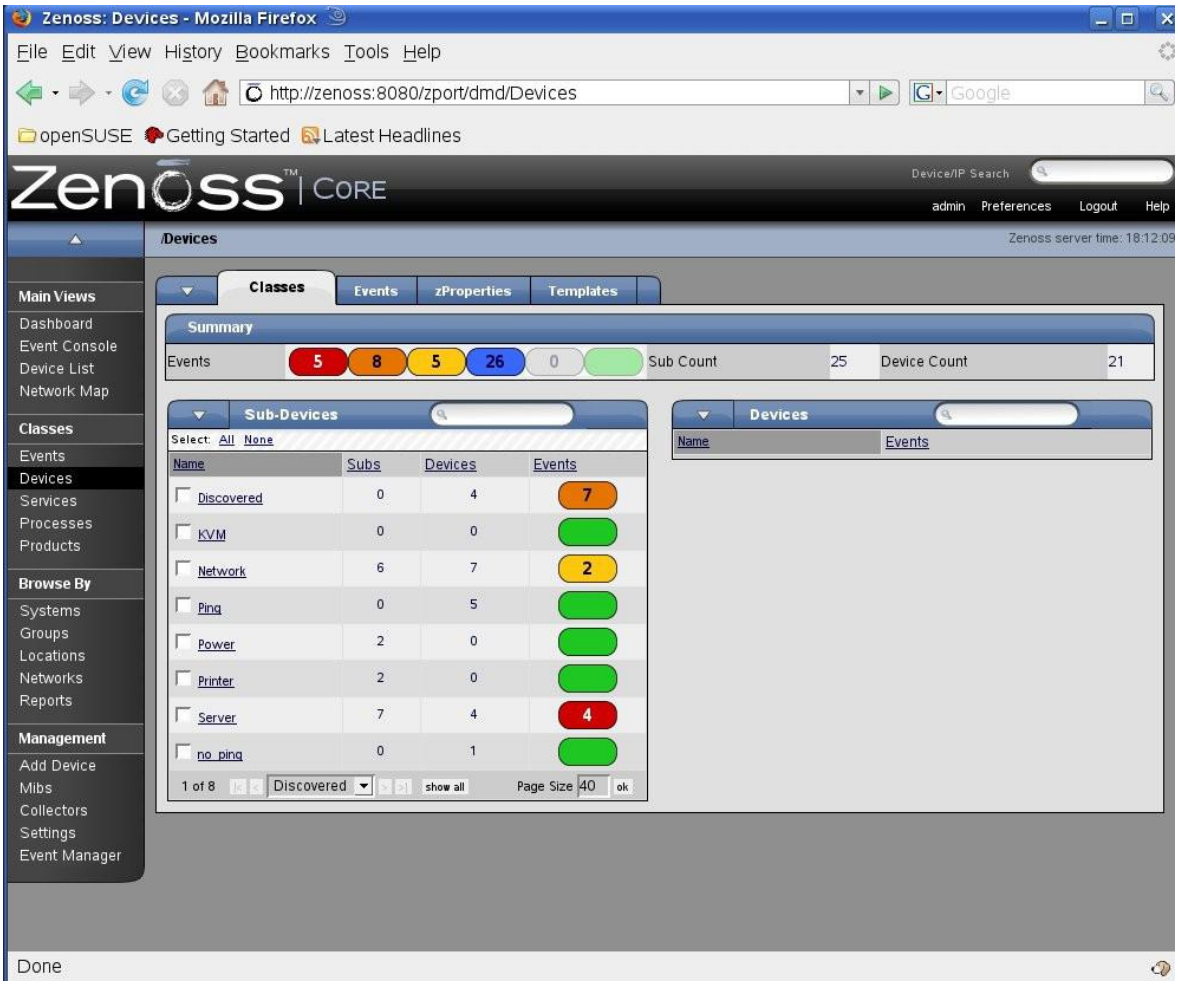


Figura 12 Visualização da opção Devices no menu Classes

Ao descobrir os dispositivos podemos mover para diferentes categorias, que estão divididas em várias classes disponíveis ou criar novas, de forma a agrupar os dispositivos para serem identificados mais facilmente. A descoberta e a monitorização são controladas por uma enorme combinação de propriedades (zProperties) aplicadas aos dispositivos. Por exemplo no caso de usar SNMP é necessário configurar os parâmetros nas zProperties.

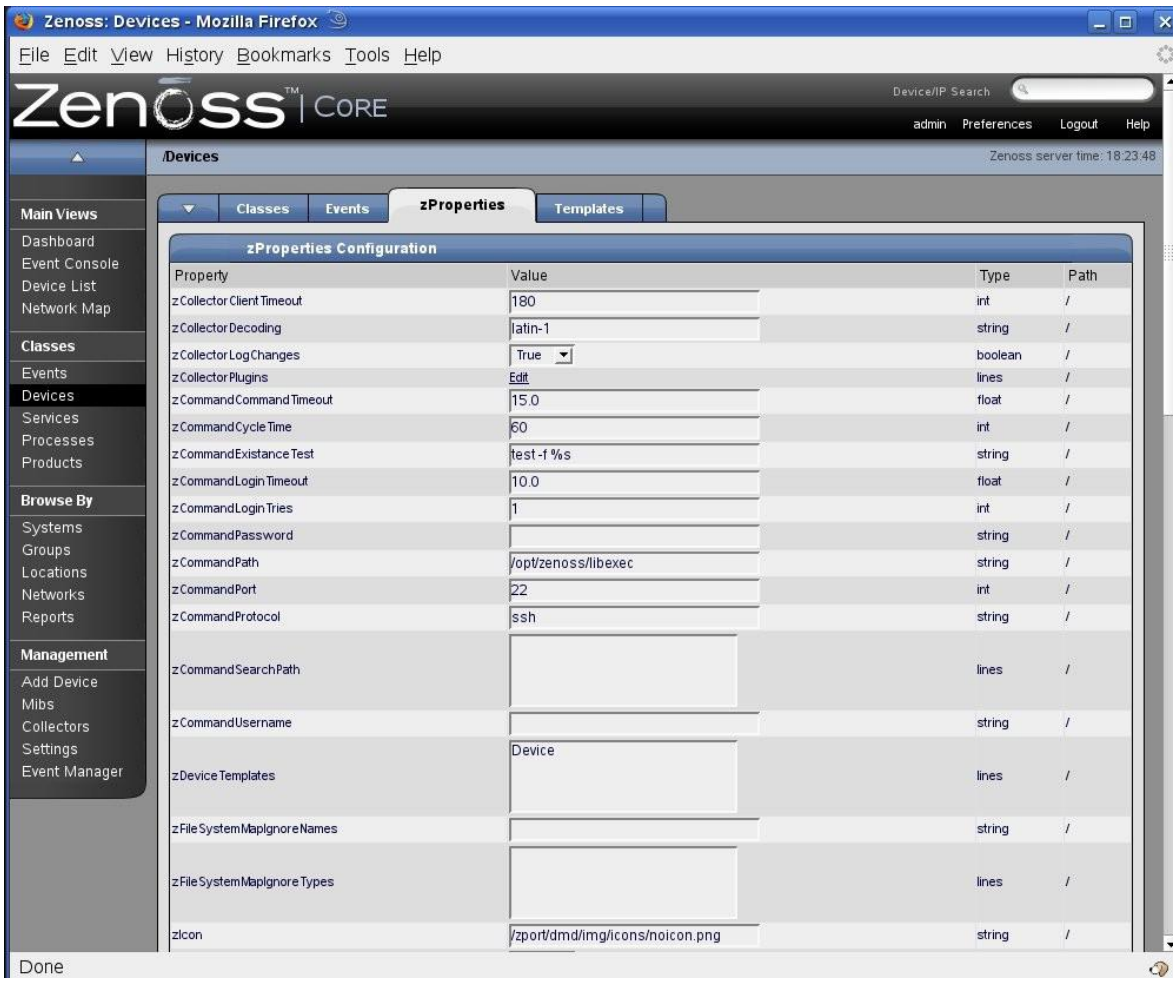


Figura 13 zProperties da classe Devices (parte 1)

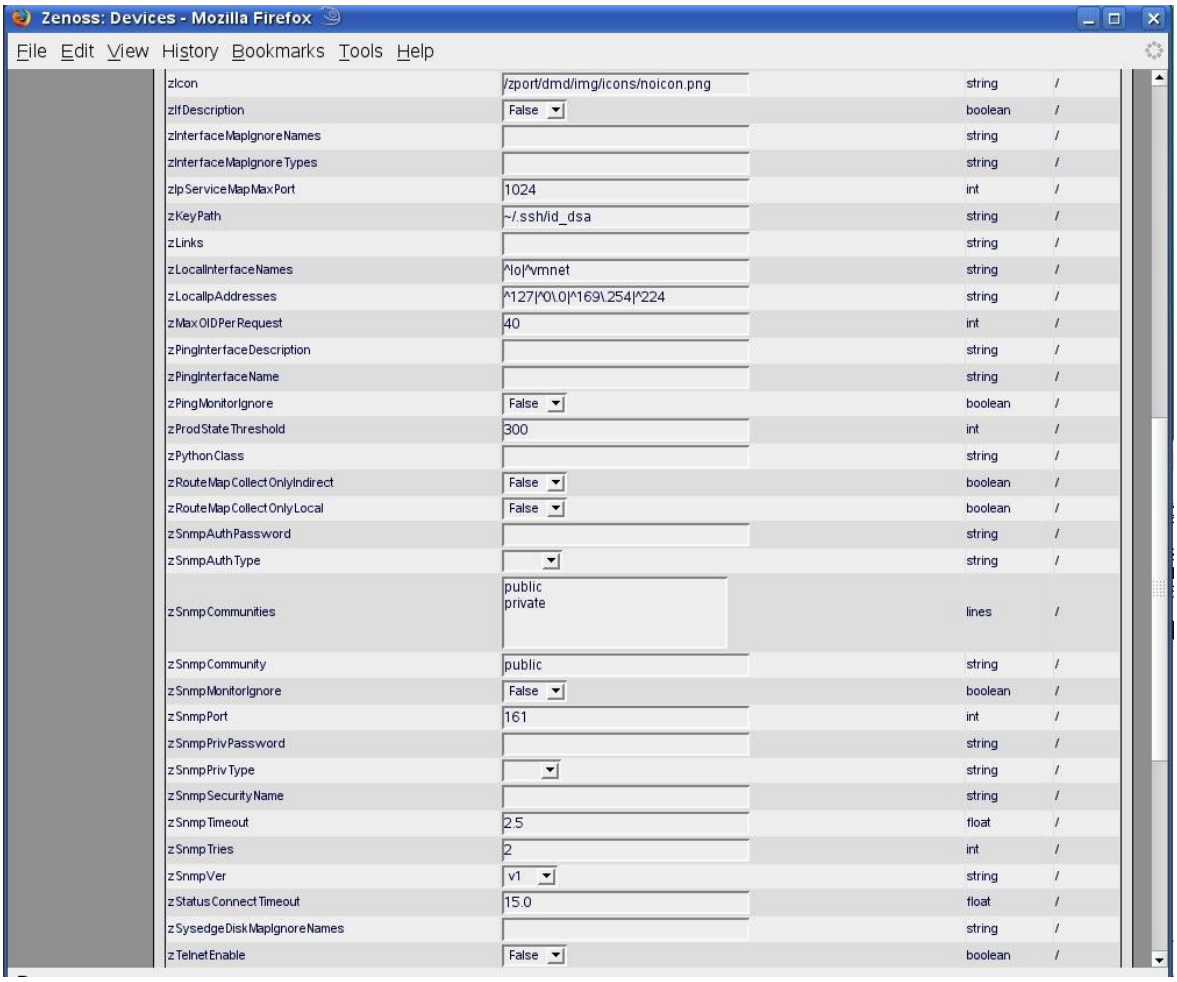


Figura 14 zProperties da classe Devices (parte 2)

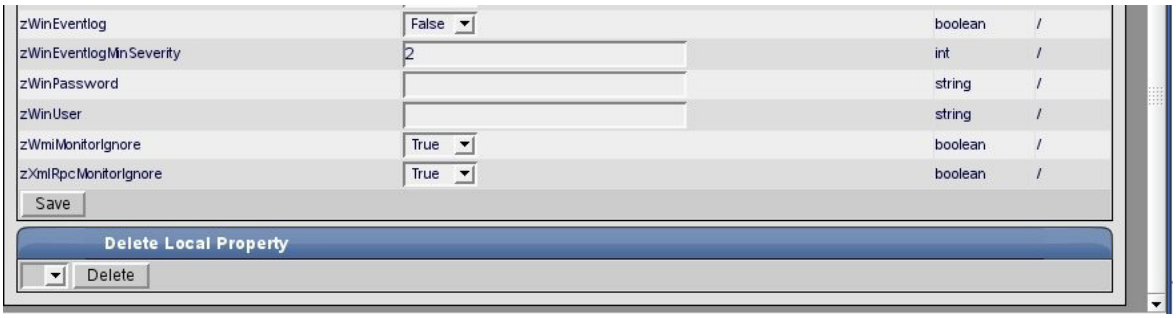


Figura 15 zProperties da classe Devices (parte 3)

3.3.3 GESTÃO DE EVENTOS

Os eventos podem ser visualizados na barra de menu Events. Existem três tipos de eventos, New, Acknowledged e Supressed. Os eventos New, são eventos recentes em que o administrador ainda não os identificou, os eventos Acknowledged são eventos que estão a ser analisados pelo administrador, e por fim os eventos Supressed, são eventos que já

foram revistos e corrigidos. Podemos facilmente verificar que é possível filtrar os diferentes tipos de eventos, bem como o seu grau de gravidade e o número de vezes em que ocorreu o evento.

3.3.4 GESTÃO DE ALERTAS

Para definir alertas no Zenoss é preciso selecionar a opção *Advanced* na barra menu, e selecionar *Alerting rules* no painel do lado esquerdo, onde vai ser possível ao utilizador configurar as regras desse alerta.

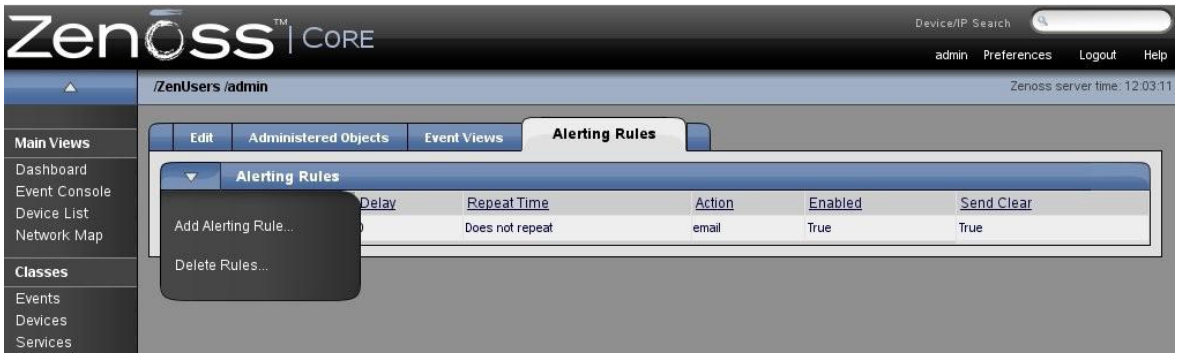


Figura 16 Menu para criar regras de alertas

Diferentes regras podem ser aplicadas consoante o grau de gravidade, estado do evento, etc. Existem seis graus de gravidade e cinco estados:

Tabela 1 Campos de gravidade

Número	Nome	Cor
0	Clear	Verde
1	Debug	Cinzento
2	Info	Azul
3	Warning	Amarelo
4	Error	Laranja
5	Critical	Vermelho

Campos de estado

- Production
- PreProduction
- Test
- Maintenance
- Decommissioned

Por omissão quando é adicionado um dispositivo, este é colocado no estado de Production, sendo este estado o mais crítico, o utilizador deve qualificar o dispositivo segundo os vários estados disponíveis.

Podemos definir o número de segundos que o alerta deve esperar até ser enviado, habilitar o alerta selecionando Enable, definir o tempo em que o alerta vai ser repetido até passar ao estado de Acknowledged, receber o alerta por email/sms. O utilizador deve definir também em que eventos, grau de gravidade, estado, o alerta deve ocorrer que por omissão estão definidos para New, Error, Production.

3.4 REFERÊNCIAS

As referências documentais…

3.5 ANEXOS

Devem ser colocados em anexo….

4. COMPARAÇÃO ENTRE NAGIOS E ZENOSS

Neste capítulo será feita uma análise no que respeita a software NMS *opensource*, fazendo uma comparação e abordando as vantagens/desvantagens do Nagios e Zenoss.

O Nagios é um produto mais antigo, ambos foram desenvolvidos para usar SNMP e o Zenoss usa este protocolo por omissão. Ambos permitem outras alternativas. Zenoss suporta ssh e telnet juntamente com os ZenPacks personalizados, o Nagios tem agentes NRPE e NSCA. Ambos têm a gestão de utilizadores, para definir utilizadores, passwords e regras. O Zenoss usa RRD Tool para mostrar informação de performance, enquanto que o Nagios não tem essa capacidade. Apesar de dependerem do SNMP, nenhum deles têm uma MIB Browser, para selecionar MIBs na recolha de informação de performance dos dispositivos.

4.1 COMPARAÇÃO DE FUNCIONALIDADES

As seguintes tabelas comparam os dois produtos nas mais básicas funcionalidades (OOTB).

4.1.1 DESCOBERTA

Tabela 2 Deteção – Nagios VS Zenoss

	Nagios	Zenoss
Descoberta Automática	Não	Sim, rede e dispositivos
Descoberta de Interfaces (eth0,f0/0,etc)	Possível através do ficheiro de configuração	Sim, incluindo as portas do switch
Descoberta de dispositivos que não suportem PING	Sim, usar o plugin check_ifstatus	Sim, usa SNMP, ssh ou telnet
SQL Base de dados	Não	MySQL & Zope ZEO
Descoberta de aplicações	Sim, define serviços	Sim, com ssh, zenpacks ou plugins
Versões SNMP	V1, 2 & 3	V 1, 2 & 3

4.1.2 DISPONIBILIDADE DE MONITORIZAÇÃO

Tabela 3 Disponibilidade de Monitorização – Nagios Vs Zenoss

	Nagios	Zenoss
Monitorização via PING	Sim	Sim
Alternativas ao PING	Sim, é possível usar plugins	Sim, ssh, telnet, ZenPacks,

	, ex: check_ifstatus	plugins do Nagios
Port Sniffing	Sim	Sim
Monitorização de Processos	Sim, com plugins	Sim, Host Resources MIB
Tecnologia "Agentes"	Geralmente depende dos plugins implementados pelo Nagios	SNMP, cliente ssh, WMI para Windows, implementação de ZenPacks
Relatórios de disponibilidade	Sim	Sim

4.1.3 GESTÃO DE EVENTOS

Tabela 4 Gestão de problemas – Nagios Vs Zenoss

	Nagios	Zenoss
Consola de eventos configurável	Não	Sim
Configuração de eventos	Sim	Flexível, Possíveis configurações OOTB
Manipulação de SNMP TRAPs	Não	Flexível, Possíveis configurações OOTB
Notificação via email/sms	Sim	Sim
Dependências serviços/ dispositivos	Sim	Não

4.1.4 GESTÃO DE PERFORMANCE

Tabela 5 Gestão ded Performance – Nagios Vs Zenoss

	Nagios	Zenoss
Recolha de informação de performance através de SNMP	Não	Sim
Recolha de informação de performance usando outros métodos	Não	SSH, Telnet, outros métodos usados por ZenPacks
Informação Threshold de performance	Não	Yes
Gráficos de informação de performance	Não	Sim, vários fornecidos OOTB
MIB Browser	Não	Sim, a partir da versão 2.2

4.2 VANTAGENS DE DESVANTAGENS DOS PRODUTOS

Nesta secção será feita uma análise, evidenciando os pontos fortes e fracos do Nagios e do Zenoss.

4.2.1 NAGIOS – VANTAGENS E DESVANTAGENS

Tabela 6 Vantagens e desvantagens do Nagios

Vantagens	Desvantagens
Código estável para sistemas de gestão	Não tem descoberta automática

Boa correlação entre eventos de serviço e de eventos de dispositivos	Fraca consola de eventos
Existência de um comando para verificar a validação dos ficheiros de configuração	Não recolhe informação de performance
Existência de um comando que faz o "reload" dos ficheiros de configuração sem interromper o Nagios	Difícil de receber e interpretar SNMP TRAPs
Boa documentação	Sem MIB Browser

4.2.2 ZENOSS – VANTAGENS E DESVANTAGENS

Tabela 7 Vantagens e desvantagens do Zenoss

Vantagens	Desvantagens
Boas funcionalidades OOTB	Sem correlação entre eventos de serviços e eventos de dispositivos
Enorme variedade de plugins & ZenPacks disponíveis	Sem MIB Browser até á versão 2.2
Notificações de email incluem links URL a direcionar para o Zenoss	Sem possibilidade de alterar as cores dos eventos
Versão comercial disponível	Versão comercial disponível
Boa documentação inicial para quem está a começar a desenvolver	Falta de informação, quando queremos informação sobre algum mais específico
Suporta plugins do Nagios	

4.3 CONCLUSÕES

Para sistemas de gestão com pouco grau de complexidade, o Nagios comporta-se eficazmente, sendo este confiável visto ter uma enorme comunidade por trás. Para testes que exigem pouco mais do que um simples PING, ou alguns testes recorrendo ao SNMP, tendo em conta que vai ser necessário instalar plugins remotos nos dispositivos, escolheria o Nagios. Apesar de a configuração de notificações ser fácil, se quisermos produzir uma análise no nosso evento então o Nagios não será a melhor opção. O Zenoss é um produto extremamente competente, detetando automaticamente os dispositivos, conseguindo obter bons gráficos de performance, tem uma boa gestão de eventos, que torna a vida mais simplificada ao utilizador. Consegue monitorizar os *system logs*, estes ficheiros contêm eventos que são escritos pelo sistema operativo de sistemas Unix, Linux, Windows, entre outros, de forma a ajudar o utilizador a perceber o que se está a passar na sua máquina.

A minha escolha vai recair pelo Nagios, devido a ter uma documentação e uma comunidade grande de utilizadores, ter a possibilidade de obter um gráfico por omissão de disponibilidade dos dispositivos (ex. saber em que dia, hora, o dispositivo foi *down* ou *up*, que foi um dos requisitos fundamentais da Nonius) e também a Nonius já tem projetos desenvolvidos com o software Nagios.

5. ESTRUTURA DA REDE

Neste capítulo apresenta-se uma breve descrição da estrutura da rede de dados a ser monitorizada (Douro Azul) assim como os aspetos previstos para aceder á rede do Douro Azul através da rede da Nonius utilizando VPN (*Virtual Private Network*).

5.1 REDE LAN DA NONIUS

A estrutura de rede da Nonius está representada na figura seguinte:

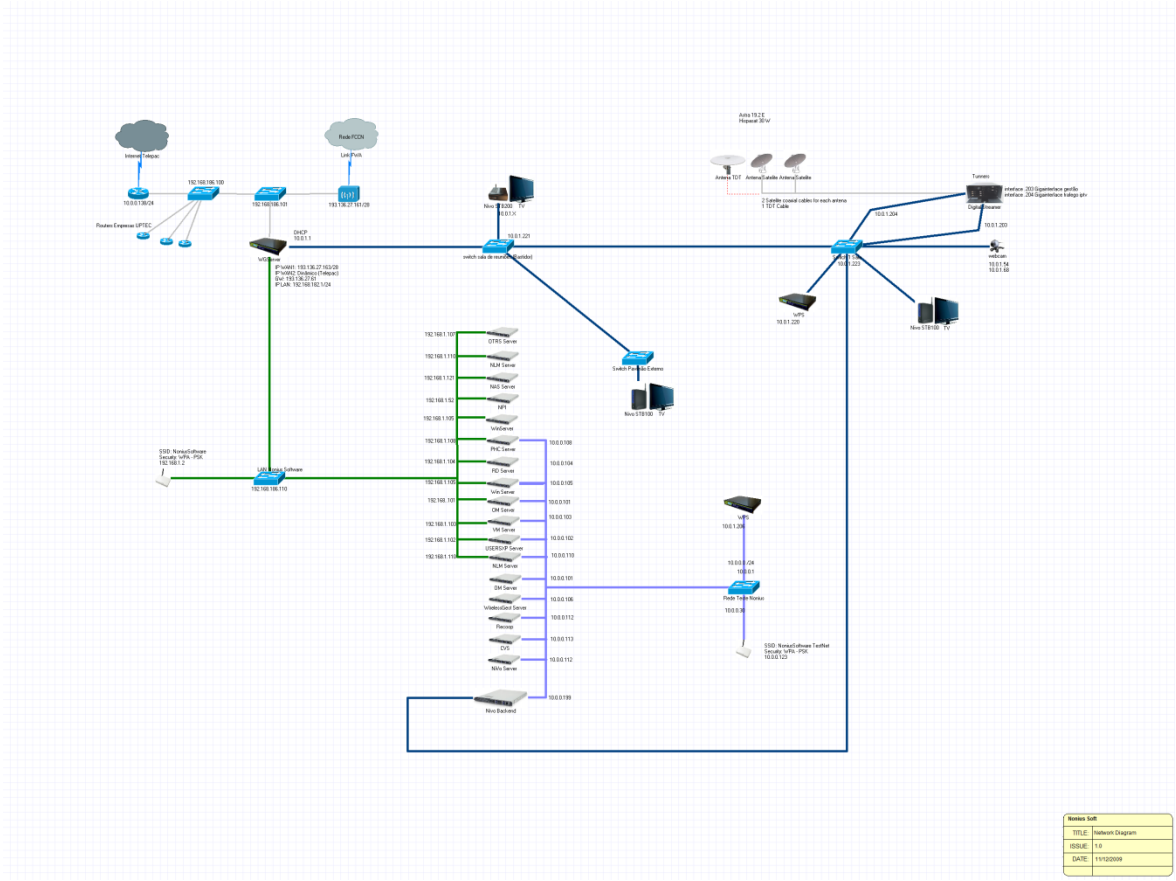


Figura 17 Mapa da rede LAN da Nonius

Para desenvolver este trabalho, foi instalado num servidor (10.0.0.171) o VMware ESXi, sendo possível criar várias máquinas virtuais. Criei uma máquina virtual e instalei o Ubuntu Server 12.04 com o endereço 10.0.0.126. Para fazer a monitorização dos dispositivos teria de ter acesso ao servidor (10.0.0.117) onde estão criados vários túneis, onde é possível fazer o suporte aos diversos clientes. Para tal foi definida as permissões devidas para que tivesse acesso apenas ao túnel do Douro Azul.

O objetivo final era ter uma ligação VPN – site-to-site para aceder á rede do Douro Azul, como na figura seguinte ilustra.

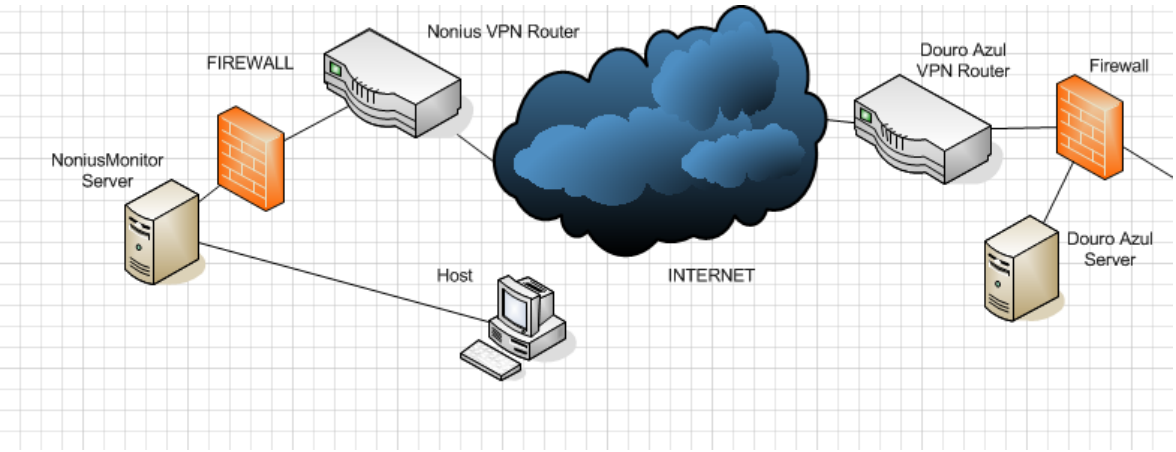


Figura 18 Interligação da rede Nonius e Douro Azul

5.2 ESCOLHA DE ROUTER PARA LIGAÇÃO VPN

A Nonius como tem vários equipamentos, foi verificar se tinham suporte para ligações VPN. Verifiquei que apenas tem disponíveis routers da ZyXEL com o modelo NBG-41X N. Toda a gama dos routers NBG-41X N, têm suporte para VPN pass-through podendo usar os protocolos (IPSec, PPTP). A funcionalidade VPN pass-through, ou seja, apenas deixa passar tráfico, não permite configurar o router como VPN server ou estabelecer uma ligação VPN site-to-site com outro router VPN.

A gama Zyxel ZyWall já oferece outro tipo de funcionalidades, como suporte para ligações VPN, filtrar páginas Web, Ipv6, etc. Neste gama o mais acessível é o ZyWALL USG 20 Firewall 5 com o preço a rondar os €160.

Outra solução possível era o router da Cisco RV180 VPN Router por volta dos €130, que oferecia características semelhantes ao Zyxel ZyWall.
Também podia-se optar por soluções wireless, optando pelos modelos:

Cisco RV110W – €80

Cisco RV120W - €140

A minha escolha seria entre routers da Cisco RV180 ou RV110 pois cumprem com todas as funcionalidades para o desenvolvimento deste trabalho, e são os mais económicos. A principal diferença entre eles são:

RV180 – VPN (IPSec,PPTP); Portas gigabit; Wired;

RV110W- VPN(PPTP, não tem IPSec) ; Portas fast ethernet; Wireless;

6. APLICAÇÃO DE GESTÃO DESENVOLVIDA

Neste capítulo será identificada todas as fases de desenvolvimento desta aplicação, descrevendo ao pormenor as diversas etapas e problemas que foram ocorrendo.

4.1 INSTALAÇÃO NAGIOS

Para proceder á instalação utilizei a versão do Ubuntu Server 12.04 e segui um guião de instalação no site do Nagios, no qual passo a descrever todos os seus passos.

Instalação de todos os pacotes necessários para que a instalação seja bem-sucedida.

```
# sudo apt-get install apache2
# sudo apt-get install libapache2-mod-php5
# sudo apt-get install build-essential
# sudo apt-get install libgd2-xpm-dev
```

Criação de uma conta utilizador com o nome nagios e definição da sua password

```
# sudo -s
# /usr/sbin/useradd -m -s /bin/bash nagios
```

```
# passwd nagios
```

Criação de um novo grupo (nagcmd) para permitir a certos comandos externos serem submetidos através da interface web. Adicionar tanto o utilizador nagios e o utilizador apache para o grupo.

```
# /usr/sbin/groupadd nagcmd

# /usr/sbin/usermod -a -G nagcmd nagios

# /usr/sbin/usermod -a -G nagcmd www-data
```

Criar uma directória para armezar downloads.

```
# mkdir ~/downloads

# cd ~/downloads
```

Fazer o download do Nagios e dos seus plugins (http://www.nagios.org/download/).

```
# wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-
3.4.1.tar.gz

# wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-
plugins-1.4.16.tar.gz
```

Extração do Nagios

```
# cd ~/downloads

# tar xzf nagios-3.4.1.tar.gz

# cd nagios-3.4.1
```

Executar o script de configuração, passando o nome do grupo criado anteriormente

```
# ./configure --with-command-group=nagcmd
```

Compilar o Nagios

```
# make all

# make install

# make install-init

# make install-config

# make install-commandmode
```

Editar o ficheiro de configuração */usr/local/nagios/etc/objects/contacts.cfg* e alterar a diretiva email e submeter o email do administrador para receber alertas.

```
# vi /usr/local/nagios/etc/objects/contacts.cfg
```

Configurar a interface-web

```
# make install-webconf
```

Criar credenciais para ter acesso á interface-web

```
# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Reiniciar o Apache

```
# /etc/init.d/apache2 reload
```

Extracção e instalação dos Nagios plugins

```
# cd ~/downloads
# tar xzf nagios-plugins-1.4.16.tar.gz
# cd nagios-plugins-1.4.16
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios
# make
# make install
```

Configurar o Nagios para automaticamente iniciar quando o máquina reinicia

```
# ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

Verificar se os ficheiros de configuração estão de acordo com as especificações

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Se não houver erros, podemos iniciar finalmente o Nagios

```
# /etc/init.d/nagios start
```

Aceder ao Nagios por interface-web

```
http://localhost/nagios/
```

4.2 CONFIGURAÇÃO DE DISPOSITIVOS E SERVIÇOS

Para começar a configurar o nagios foi feita uma recolha de dispositivos instalados na frota Douro Azul. Seguidamente apresentarei os dispositivos a serem monitorizados em cada navio.

Tabela 8 Dispositivos instalados nos diversos navios

Navio	Nº APs	Nº Switchs	Nº Voip Server	Nº WGServer	Nº NiVo
Alto Douro	2	x	x	1	x
Douro Queen	11	x	x	1	x
Douro Prince	3	x	x	1	x
Douro Cruiser	8	x	x	1	x
Douro Spirit	5	6	1	1	1

4.3 ACEDER REMOTAMENTE A DISPOSITIVOS – NRPE PLUGIN

Surgiu a necessidade de monitorizar remotamente diversas máquinas, essencialmente dispositivos ligados ao WGServer, pretende-se monitorizar todos os dispositivos que estejam conectados ao WGServer (APs, SWs, Voip, etc) e a solução encontrada foi com o plugin *NRPE* do Nagios.

O *NRPE* (daemon e plugin) estabelece a comunicação entre o servidor Nagios e a máquina Linux/Unix remota, a ser monitorizada. Este usará um canal SSL para uma comunicação segura entre o servidor Nagios e seus clientes Linux/Unix.

O NRPE é um complemento para o Nagios e foi criado para possibilitar a monitorização de máquinas remotas Linux/Unix. Em outras palavras, o complemento NRPE é desenvolvido de forma a permitir que sejam executados os plugins do Nagios em máquinas Linux/Unix, permitindo ao gestor monitorizar uma máquina Linux/Unix, bem como ser capaz de "monitorizar" outras máquinas na rede, num esquema de validações indiretas.

O NRPE é um agente que trabalha numa máquina remota com o objetivo exclusivo de colecionar informações e enviá-las ao servidor Nagios. A figura abaixo exemplifica o processo de comunicação entre o servidor Nagios e um cliente por meio do NRPE. Sendo esta comunicação protegida por SSL.

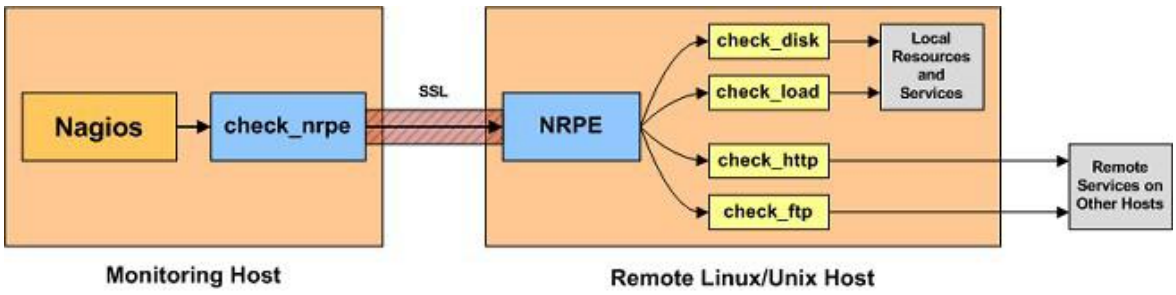


Figura 19 Comunicação do Nagios com um cliente via NRPE

O NRPE é composto por:

- Daemon NRPE, é um agente ativo que fica no sistema a monitorizar e se encarrega das requisições e coleção dos dados do mesmo.

- Plugin check_nrpe, instalado no servidor Nagios.

Para que seja possível realizar uma instalação correta, é de maior importância que se entenda como o processo de comunicação entre o servidor Nagios (por meio do plugin check_nrpe) e o cliente Linux/Unix monitorizado (cujo daemon NRPE está instalado) trocam informações.

Quando o Nagios precisa de monitorizar um recurso ou serviço numa máquina Linux/Unix remota, segue resumidamente os seguintes passos:

- Executará o plugin check_nrpe, dizendo qual o serviço deverá ser validado;

- O plugin, então, contata o daemon NRPE na máquina remota, sob uma conexão protegida por SSL;
- O daemon NRPE corre o plugin apropriado para validar o serviço, ou recurso, requerido;
- Os resultados obtidos são passados pelo daemon NRPE de volta ao plugin check_nrpe, que então retorna os resultados para o processo do Nagios que, eventualmente, os mostrará em sua interface web.

Instalação do NRPE na máquina remota,

Criar conta de utilizador Nagios,

```
# su -l
# /usr/sbin/useradd nagios
# passwd nagios
```

Instalar e compilar plugins do Nagios,

```
# mkdir /downloads
# cd /downloads

# wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-#
plugins-1.4.16.tar.gz
# tar xzf nagios-plugins-1.4.16.tar.gz
# cd nagios-plugins-1.4.16

# ./configure
# make
# make install
```

Dar permissões de acesso à conta "nagios",

```
# chown nagios.nagios /usr/local/nagios
# chown -R nagios.nagios /usr/local/nagios/libexec
```

Instalar o xinetd,

```
apt-get install xinetd
```

Instalar, extrair e compilar o daemon NRPE,

```
# cd /downloads
# wget http://sourceforge.net/projects/nagios/files/nrpe-2.x/nrpe-
2.13/nrpe-2.13.tar.gz

# tar xzf nrpe-2.13.tar.gz
```

```
# cd nrpe-2.13

# ./configure
# make all

# make install-daemon
# make install-daemon-config
```

Instalar o daemon NRPE como um serviço que corre sobre o xinetd,

```
# make install-xinetd
```

Editar o arquivo */etc/inetd.d/nrpe* e adicione o IP do servidor de monitorização (Nagios) à diretiva 'only-from'. Está diretiva pode conter múltiplos endereços IP, passados entre espaços. Este exemplo permite acesso ao servidor de monitorização à máquina local,

```
# vi /etc/xinetd.d/nrpe
```

```
...
only_from = 127.0.0.1 <endereço IP do Nagios>
...
```

Adicionar o texto abaixo, para o daemon do NRPE, no ficheiro */etc/services*,

```
# vi /etc/xinetd.d/nrpe
```

```
...
nrpe       5666/tcp # porta NRPE (Nagios Remote Plugin Executor)
...
```

Reiniciar o serviço xinetd,

```
# service xinetd restart
```

Certificar que a firewall permite dar acesso ao daemon NRPE para o(s) servidor(es) de monitorização, e somente para ele(s). Alterar as regras do iptables na linha de comando.

```
# iptables -A INPUT -p tcp --dport 5666 -j ACCEPT
```

Testar se o daemon NRPE está a correr localmente,

```
# netstat -at | grep nrpe
```

O output deverá ser o seguinte,

```
# tcp 0 0 *:nrpe *:* LISTEN
```

Seguidamente é preciso validar o daemon NRPE para ter a certeza que está a funcionar corretamente,

```
# /usr/local/nagios/libexec/check_nrpe -H localhost
```

Devemos ter como output a versão do NRPE,

```
#NRPE v2.13
```

O ficheiro de configuração do NRPE, possui muitas definições de comandos para que seja possível monitorizar a máquina. Para alterar as definições existentes, inserir novos comandos, etc, basta editar o ficheiro de configuração do NRPE,

```
# vi /usr/local/nagios/etc/nrpe.cfg
```

Podemos testar alguns deles recorrendo os seguintes comandos:

```
# /usr/local/nagios/libexec/check_nrpe -H localhost -c check_users
# /usr/local/nagios/libexec/check_nrpe -H localhost -c check_total_procs
# /usr/local/nagios/libexec/check_nrpe -H localhost -c check_zombie_procs
```

Até aqui foi instalado e configurado o NRPE na máquina remota. Agora vamos prosseguir a instalação/configuração do plugin NRPE no servidor Nagios.

Nesta etapa, serão realizados os seguintes passos:

1. Instalar a biblioteca SSL;
2. Compilar o NRPE e instalar o plugin check_nrpe;
3. Criar definição para o uso do check_nrpe;
4. Criar uma nova definição de host para a nova máquina a ser monitorizada.

Os exemplos de configuração são demonstrados nos modelos de referência. Estes modelos são definidos nos ficheiros de exemplo: *localhost.cfg* e *commands.cfg*.

Atualizar os repositórios,

```
# apt-get update
```

Instalar a biblioteca SSL,

```
# apt-get install libssl-dev openssl
```

Instalar o plugin check_nrpe,

```
# mkidr /downloads
# cd downloads

# wget http://sourceforge.net/projects/nagios/files/nrpe-2.x/nrpe-
2.13/nrpe-2.13.tar.gz
```

Extrair os arquivos,

```
# tar xzf nrpe-2.13.tar.gz
```

```
# cd nrpe-2.13
```

Compilar o complemento NRPE,

```
# ./configure
# make all
```

Instalar o plugin NRPE,

```
# make install-plugin
```

Testar a comunicação com o daemon NRPE,

```
# /usr/local/nagios/libexec/check_nrpe -H 10.0.0.126 (servidor Nagios)
```

Como resposta, aparecerá uma string informando a versão do NRPE instalado, como o seguinte,

```
# NRPE v2.13
```

Criar uma definição no ficheiro commands.cfg
É necessário adicionar uma nova definição de comand no ficheiro de configuração do Nagios para usar o check_nrpe.

Abrir o ficheiro commands.cfg,

```
# vi /usr/local/nagios/etc/objects/command.cfg
```

Adicionar a seguinte definição para o ficheiro,

```
...
define command
{
command name check nrpe
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
...
```

Isto dirá ao Nagios que, agora, ele possui um comando chamado “check_nrpe” e que poderá executá-lo utilizando os parâmetros definidos acima.

Agora que ambas as máquinas estão configuradas, estamos aptos para configurar serviços para serem monitorizados pela máquina.

4.4 PROBLEMAS DE CONFIGURAÇÃO DO PLUGIN NRPE NO NIVOBACKEND/WGSERVER

Um dos problemas que o NRPE afetou o desenvolvimento deste trabalho foi o facto de ter que instalar os seguintes pacotes nas máquinas remotas (nivobackend e wgserver):

- Plugins do nagios - http://www.nagios.org/download/plugins/
- xinetd – apt-get install xinetd (the extended Internet services daemon)
- openssl – apt-get install libssl
- NRPE Plugin - http://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details

A versão do sistema operativo no NiVoBackend é o Ubuntu 8.10 e no WGServer é o Fedora Core 3. A instalação no NiVoBackend, segundo o tutorial acima descrito funcionou corretamente sem grandes dificuldades.
Na instalação no WGServer surgiu alguns problemas, visto este usar um sistema operativo diferente (FC3) , logo tutorial acima teria que ser algo semelhante mas para a versão Fedora em vez de Ubuntu.

Para que o NRPE funciona-se no sistema operativo Fedora Core 3, executei os seguintes passos:

- Verificar se tinha já instalado os pacotes openssl e o xinetd através do comando,
  ```
  # rpm -qa | sort > lista-pacotes.txt
  ```

- Como não tinha os pacotes instalados, fiz o download do openssl-0.9.7a.tar.gz e do xinetd-2.3.13.tar.gz manualmente

- Procedi á instalação dos mesmos com os comandos,

  ```
  # tar xvf openssl-0.9.7a.tar.gz
  # ln -s /lib/libssl.so.0.9.7a /usr/local/ssl/lib/libssl.so
  # cd openssl-0.9.7a
  # ./configure --with-ssl=/usr/local/ssl/lib
  # make
  # make install
  # cd ..
  # tar zxf xinetd-2.3.13.tar.gz
  # cd xinetd-2.3.13
  # ./configure
  # make
  # make install
  ```

- Seguidamente, recorri normalmente ao tutorial acima descrito para instalar o plugin NRPE e fazer as devidas configurações.

7 CONCLUSÃO

Neste capítulo apresenta-se o balanço do trabalho descrito ao longo deste relatório, e estudos e implementações futuras.

O objectivo do estágio numa primeira fase era estudar as diversas tecnologias *opensource* para sistemas de gestão de redes (NMS) para que seja realizada uma monitorização aos vários dispositivos instalados nos navios na frota Douro Azul. Para tal foi feito um estudo sobre os programas Nagios e Zenoss. Para sistemas de gestão com pouco grau de complexidade, o Nagios comporta-se eficazmente, sendo este confiável visto ter uma enorme comunidade por trás. Para testes que exigem pouco mais do que um simples PING, ou alguns testes recorrendo ao SNMP, tendo em conta que vai ser necessário instalar plugins remotos nos dispositivos, escolheria o Nagios. Apesar de a configuração de notificações ser fácil, se quisermos produzir uma análise no nosso evento então o Nagios não será a melhor opção. Relativamente ao Zenoss, é um produto extremamente competente, detetando automaticamente os dispositivos, conseguindo obter bons gráficos de performance, tem uma boa gestão de eventos, que torna a vida mais simplificada ao utilizador. Consegue monitorizar os ficheiros *system logs*, que contêm eventos escritos pelo sistema operativo de sistemas Unix, Linux, Windows, entre outros, de forma a ajudar o utilizador a perceber o que se está a passar na sua máquina. A minha escolha vai recair pelo Nagios, devido a ter uma boa documentação e uma comunidade grande de

utilizadores, ter a possibilidade de obter um gráfico por omissão de disponibilidade dos dispositivos (ex. saber em que dia, hora, o dispositivo foi *down* ou *up*, que foi um dos requisitos fundamentais da Nonius).

Numa segunda fase adquiri conhecimentos sobre o programa Nagios para implementar o desenvolvimento deste trabalho. Tais como, instalação, configurar diversos dispositivos e serviços, notificações e monitorizar máquinas remotas. No que respeita á instalação, existe boa documentação no site oficial do Nagios que permite de forma simples e concisa perceber que comandos estão a ser executados ao longo da sua instalação.

Finalizada a instalação e como o Nagios não descobre dispositivos automaticamente, foi necessário configurar os dispositivos manualmente, ora no Nagios essa configuração é feita com base em ficheiros, quer para dispositivos, quer para serviços. Podemos monitorizar vários tipos de serviços, por exemplo SMTP, POP3, HTTP, ICMP, SNMP. É possível configurar diversos administradores no ficheiro *contacts.cfg* de forma a receber notificações por email no caso de ocorrer eventos críticos, ou seja, quando algum dispositivo/serviço deixa de funcionar corretamente. Para monitorizar máquinas remotas utilizei o plugin *NRPE* do Nagios que permite trocar informação com o servidor e a máquina remota (Unix/Linux) sendo assim possível apresentar no servidor Nagios toda a configuração de dispositivos/serviços efetuada na máquina remota.

Para aceder remotamente aos dispositivos estava previsto estabelecer uma ligação VPN – Site-to-Site e foi feita uma análise de equipamentos possíveis. Este procedimento ficou em stand-by e para ter acesso aos equipamentos foi-me dado acesso ao túnel através da máquina nemesis (10.0.0.117) para aceder á rede da frota azul (10.9.0.0/23).

Histórico

- 31 de Outubro de 2007, Versão 1.0, mailto:pfa@isep.ipp.pt
- 2 de Novembro de 2007, Versão 1.0a, mailto:pfa@isep.ipp.pt
- 16 de Novembro de 2007, Versão 1.0b, mailto:pfa@isep.ipp.pt

$Id:MEEC-TEDI.dot v1.0b Date:16-11-2007$