UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
ESCOLA DE INFORMÁTICA APLICADA

MONITORAMENTO DA REDE UNIRIOTEC ATRAVÉS DA FERRAMENTA CENTREON

JOÃO MARCELLO CALIL VAZ MENEZES SANTANA DE LIMA

Orientador
SIDNEY CUNHA DE LUCENA

RIO DE JANEIRO, RJ – BRASIL
DEZEMBRO DE 2016

MONITORAMENTO DA REDE UNIRIOTEC ATRAVÉS DA FERRAMENTA CENTREON

JOÃO MARCELLO CALIL VAZ MENEZES SANTANA DE LIMA

Projeto de Graduação apresentado à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) para obtenção do título de Bacharel em Sistemas de Informação.

Aprovada por:

_____

SIDNEY CUNHA DE LUCENA (UNIRIO)

_____

MORGANNA CARMEM DINIZ (UNIRIO)

_____

CARLOS ALBERTO VIEIRA CAMPOS (UNIRIO)

RIO DE JANEIRO, RJ – BRASIL.

DEZEMBRO DE 2016

Agradecimentos

À minha família e aos professores que me lecionaram, por toda a base criada e todo o auxílio prestado para moldar meu caráter e meu conhecimento.

Aos amigos com os quais dividi sabores e dissabores desta trajetória acadêmica, pelo companheirismo que me ajudou a não desistir nos momentos de fraqueza.

Ao professor Carlos Eduardo Fraga Ribeiro, da escola online FAME Treinamentos, cujo curso me permitiu obter um grande conhecimento sobre o sistema Centreon, elemento primordial deste trabalho.

À Escola de Informática Aplicada, que forneceu o ambiente possível para a realização deste trabalho e à qual pretendo deixar um legado na forma do sistema implementado.

RESUMO

Este trabalho mostrará a inserção de um sistema de monitoramento de redes na infraestrutura computacional pertencente à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro (UNIRIO), localizada no Centro de Ciências Exatas e Tecnologia (CCET) da referida universidade. Serão apresentados também a importância de se utilizar o monitoramento de redes e como este funciona, bem como alguns dos principais sistemas que o aplicam, incluindo o sistema a ser instalado. Por fim, será também apresentada uma análise dos dados coletados por este sistema, feita com o objetivo de avaliar o comportamento de alguns dos servidores pertencentes à rede de computadores da universidade.

Palavras-chave: Monitoramento, redes, Centreon

ABSTRACT

This work will show the insertion of a network monitoring system into the network infrastructure belonging to the School of Applied Informatics of the Federal University of the State of Rio de Janeiro (UNIRIO). located within the Center of Exact Sciences and Technology of the aforementioned university. The importance of using network monitoring systems will also be presented, as well as some of the main systems that are used to apply it. The work will be concluded with an analysis of the data collected by this system, made with the goal of evaluating the behavior of some of the servers that belong to the university's computer network.

Keywords: Monitoring, networks, Centreon

SUMÁRIO

ÍNDICE DE FIGURAS

LISTA DE SIGLAS

UNIRIO – Universidade Federal do Estado do Rio de Janeiro

CCET – Centro de Ciências Exatas e Tecnologia

EIA – Escola de Informática Aplicada

BSI – Bacharelado em Sistemas de Informação

VPN – Virtual Private Network

FTP – File Transfer Protocol

RAM – Random Access Memory

CPU – Central Processing Unit

SNMP – Simple Network Management Protocol

BRISA – Sociedade Brasileira para Interconexão de Sistemas Abertos

VNC – Virtual Network Computing

AOL – America OnLine

RRD – Round Robin Database

1 Introdução

1.1 Motivação

Nos dias de hoje, é extremamente raro, senão impossível, encontrar uma organização completamente independente da computação. Sistemas computacionais são utilizados em larga escala no mundo corporativo, sendo tanto um fim como um meio; há uma vasta quantidade de empresas que desenvolvem sistemas ou especializam-se na utilização de sistemas já existentes. Dentro deste contexto, também se fazem extremamente presentes as redes de computadores, que ampliam muito as possibilidades de utilização da computação. Funcionalidades que possuem redes como base - acesso remoto a dados e aplicações, bancos de dados, conexões via VPN[1], o simples acesso a sites da Internet, dentre outros - desempenham um papel essencial dentro de uma grande quantidade de organizações.

Porém, o simples fato de uma organização possuir o máximo possível de funcionalidades de rede dentro das possibilidades de auxílio às tarefas desempenhadas não é o suficiente para se desempenhar satisfatoriamente todas as tarefas durante todo o tempo. Para que as atividades corporativas sejam efetuadas com a mínima quantidade possível de contratempos (como, por exemplo, longos períodos de indisponibilidade de conexões de Internet e ataques que ameacem a segurança dos dados armazenados localmente pela empresa), é preciso que a rede seja constantemente monitorada, de forma a se poder executar o tratamento de problemas o mais rapidamente possível - ou mesmo antes que ocorram.

O setor de infraestrutura de uma empresa é o responsável por cuidar de sua rede, colaborando para que ela esteja sempre funcionando, com o objetivo de evitar que os processos de trabalho sejam interrompidos. Neste setor, se fazem presentes as figuras dos analistas de infraestrutura e dos gerentes de rede, que trabalham em conjunto para efetuar tarefas como, por exemplo, definir quantos e quais ativos serão necessários para a construção da rede da empresa, definir as configurações de hardware e de software utilizadas nos servidores, verificar periodicamente a necessidade de mudanças e melhoras em qualquer parte da infraestrutura e estar de prontidão para a resolução de problemas que venham a ocorrer.

[1] Virtual Private Network (Rede Virtual Privada). É um modo de conexão através do qual é possível se conectar a uma rede remota para se acessar aplicações, arquivos, servidores ou itens de rede nela contidos como se o usuário estivesse conectado a ela de forma presencial.

Para que esta última tarefa seja facilitada, a empresa pode decidir, juntamente a seu setor de infraestrutura, pela utilização de sistemas de monitoramento, que possuem a função de auxiliar os administradores da rede na resolução rápida de ocorrências indesejadas.

A rede de computadores pertencente à Escola de Informática Aplicada (EIA) da Universidade Federal do Rio de Janeiro (UNIRIO), que abriga o curso de Bacharelado em Sistemas de Informação (BSI) da universidade, será o objeto de aplicação do estudo de caso presente neste trabalho. Atualmente, não há política de monitoramento - e esta opção da diretoria da Escola por não utilizar um sistema de monitoramento implica em não se saber mais a fundo sobre o uso das conexões, como, por exemplo, a quantidade de banda utilizada por um site ou por um sistema, e dificulta a adoção de políticas de bom uso da rede a fim de se evitar casos de sobrecarga e de lentidão nas conexões, que são os problemas mais comuns enfrentados pelo setor de infraestrutura de uma organização e podem gerar dificuldades no uso da rede por alunos e professores.

1.2 Objetivos

Dado o cenário descrito, este trabalho pretende efetuar uma profunda mudança na política de monitoramento de redes utilizada pelo CCET da UNIRIO, com o objetivo de reduzir o máximo possível de contratempos relativos às conexões de rede e melhorar o desempenho de seu setor de infraestrutura através da adoção de práticas que possibilitem maior proatividade.

O primeiro passo para este objetivo será feito através da implantação do Centreon, um sistema polivalente de monitoramento que pode ser utilizado para monitorar não somente as conexões de rede da empresa como também diversos aspectos de software e hardware dos ativos da rede (itens de rede, servidores e máquinas utilizadas pelos funcionários), na infraestrutura de rede da empresa, com o objetivo de expandir o leque de possibilidades de monitoramento e concentrar todas estas funções em um servidor local. O processo de implantação será descrito detalhadamente; sendo documentada a instalação do sistema e a configuração dos aspectos do sistema que serão importantes para o que se deseja monitorar.

Após a instalação do sistema, será fornecida uma janela de tempo para que o Centreon colete dados de tráfego em relação a alguns dos servidores presentes na rede, que serão

especificados; com os dados coletados nesta janela, será feita uma análise estatística para analisar o comportamento do tráfego de rede em relação aos servidores escolhidos.

1.3 Organização do texto

O presente trabalho está estruturado em capítulos e, além desta introdução, será desenvolvido da seguinte forma:

- Capítulo II: Será explicada a importância da utilização do monitoramento de redes em ambientes corporativos, assim como o funcionamento do SNMP, o principal protocolo de conexão utilizado por estes sistemas. Também será feita a apresentação de alguns dos sistemas de monitoramento mais conhecidos e utilizados por empresas - dentre eles o Centreon, que é o objeto do estudo de caso que será apresentado. Ao final, serão feitas comparações entre o Centreon e os sistemas apresentados.
- Capítulo III: Será apresentada uma breve história do sistema Centreon e o motivo de sua escolha para uso no presente trabalho.
- Capítulo IV: Serão apresentados a infraestrutura de rede da Escola de Informática Aplicada e o processo de inserção do Centreon nesta infraestrutura, sendo documentadas a instalação e a configuração do sistema.
- Capítulo V: Será apresentada a análise do tráfego de rede da Escola de Informática Aplicada, realizada utilizando-se os dados coletados pelo Centreon e ilustrada por gráficos.
- Capítulo VI: Conclusões – Reúne as considerações finais, assinala as contribuições da pesquisa e sugere possibilidades de aprofundamento posterior.

2 Monitoramento de redes

A fusão dos computadores e das comunicações influenciou fortemente a organização dos sistemas computacionais. Os centros de computadores, que consistiam em salas para onde eram levados os programas a serem executados através de cabeamentos ou de cartões perfurados, foram extintos há tempos; o antigo *modus operandi* em que cada organização possui uma única máquina atendendo a todas as suas necessidades computacionais foi substituído pelas redes de computadores, nas quais as tarefas são realizadas por um conjunto de estações interligadas.

Como relatado por Benini e Daibert (2011), as redes de computadores ganharam importância a partir da década de 80, especialmente devido ao barateamento dos computadores, o que tornou cada vez mais interessante a distribuição do poder computacional das organizações em módulos localizados em diversos pontos de suas estruturas. A utilização de redes de computadores não se limita somente a pesquisas por dados presentes no vasto mundo de conhecimento da Internet, estando presente também em várias atividades do cotidiano: Serviços bancários, uso de cartões de crédito, chamadas telefônicas, dentre outros serviços comumente utilizados pela sociedade. Percebe-se que, a cada dia, as pessoas possuem uma dependência maior em relação à utilização destes serviços e, por consequência, também em relação à utilização de redes.

O progresso de qualquer organização cujos serviços sejam desempenhados por computadores ou, ao menos, auxiliados por eles passa por investimentos em sua infraestrutura computacional, que é composta, basicamente, por servidores, conexões de Internet via banda larga (para tarefas comuns, como, por exemplo, acesso a sites e utilização de aplicações) ou fibra óptica (para conexões que demandem maior estabilidade, como, por exemplo, VPNs *site-to-site*[2]), equipamentos de rede (modems, roteadores, switches, hubs e pontos de acesso sem fio) e estações de trabalho (notebooks e desktops). Estes investimentos necessitam, naturalmente, de uma intensidade tão grande quanto for necessário para o bom funcionamento da organização; caso seja preciso que a organização efetue uma expansão tanto em seu escopo

[2] Modo de conexão via VPN em que duas redes estão permanentemente conectadas uma à outra, possibilitando, ao contrário do modo *client-to-site*, o acesso de qualquer máquina pertencente a uma destas redes a servidores e aplicações pertencentes à outra rede sem a necessidade de utilização prévia de uma ferramenta de conexão VPN do sistema operacional ou de softwares específicos para se efetuar a conexão.

de atividades desempenhadas (para obter uma maior polivalência de serviços e poder competir de forma mais consistente no mercado) quanto em sua estrutura física (para aumentar seu contingente de funcionários caso a estrutura atual esteja saturada), esta expansão deverá englobar também os investimentos em sua estrutura computacional. A figura 1 mostra algumas possibilidades de evolução do setor computacional de uma organização.

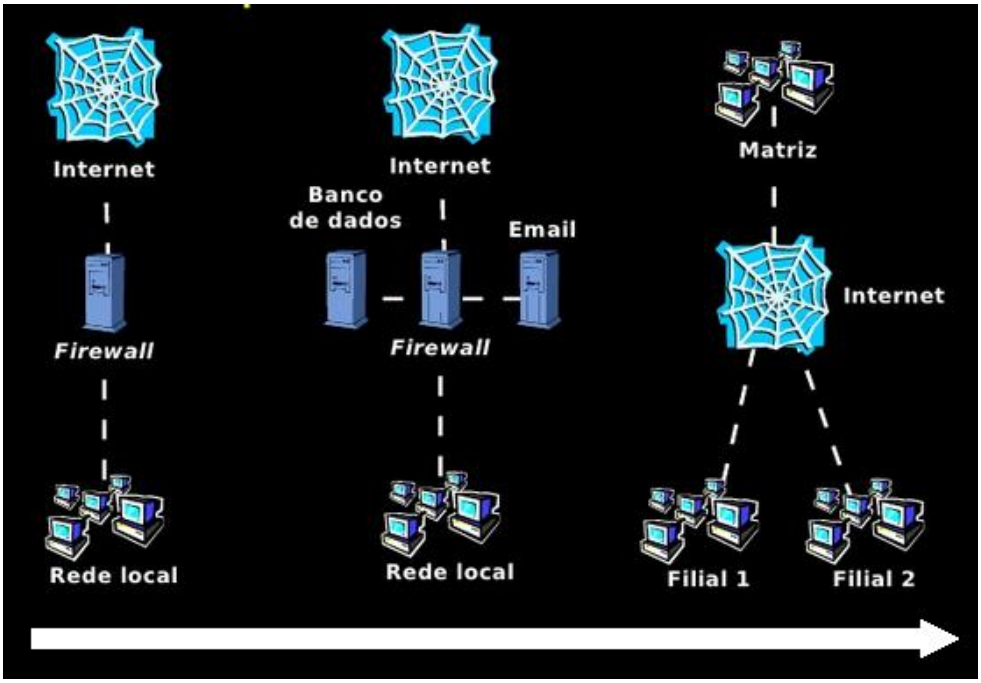

Figura 1 - Três cenários possíveis de evolução do parque computacional e da infraestrutura de uma empresa. (Adaptado de Bauermann (2010)).

Porém, ainda que uma empresa possua equipamentos de última geração e softwares em conformidade com o que há de mais avançado para uso em ambientes corporativos, é necessário ter em mente que isto não garante, por si só, o pleno funcionamento dos processos de trabalho. Qualquer componente da rede, por maior que seja seu nível de qualidade, é passível de apresentar alguma espécie de comportamento que prejudique seu desempenho, mesmo que isso só aconteça depois de um bom tempo de uso; tais comportamentos indesejáveis, se não forem tratados em tempo hábil, podem se agravar e gerar contratempos maiores.

2.1 A importância do monitoramento de redes

Um contexto histórico que permite uma compreensão inicial da importância do gerenciamento de redes - e, por consequência, da utilização de sistemas designados para auxiliá-lo - é apresentado por Kurose e Ross (2010):

> "Nos primórdios das redes de computadores, quando elas ainda eram artefatos de pesquisa, e não uma infraestrutura usada por milhões de pessoas por dia, 'gerenciamento de rede' era algo de que nunca tinha se ouvido falar. Se alguém descobrisse algum problema na rede, poderia realizar alguns testes, como o *ping*, para localizar a fonte do problema e, em seguida, modificar os ajustes do sistema, reiniciar o software ou o hardware ou chamar um colega para fazer isso. (...) Como a Internet pública e as intranets privadas cresceram e se transformaram de pequenas redes em grandes infraestruturas globais, a necessidade de gerenciar mais sistematicamente a enorme quantidade de componentes de hardware e software dentro dessas redes também se tornou mais importante." (KUROSE; ROSS, 2010)

Devido à posição fundamental que ocupam em ambientes corporativos, um dos principais problemas que podem ocorrer durante o uso de redes de computadores presentes neste tipo de ambiente (as intranets privadas mencionadas no parágrafo anterior) é a indisponibilidade. Redes de computadores instaladas em ambientes corporativos foram designadas para estarem sempre conectadas, possibilitando às aplicações que as possuem como base de funcionamento estarem sempre disponíveis para serem utilizadas; a impossibilidade ou dificuldade do uso contínuo de uma rede, tanto em forma de oscilações como em forma de quedas, tende a dificultar o cumprimento de prazos de tarefas por parte dos funcionários da organização. Quanto maior for o tempo de atraso de trabalho dos funcionários, por qualquer motivo, maior é a chance de ocorrerem problemas na relação entre a empresa e seus clientes, especialmente em casos de urgência; situações deste tipo podem até mesmo acarretar em prejuízos financeiros.

A segurança das informações da empresa também pode ser afetada por contratempos em que há o envolvimento de conexões de rede. Caso aconteça alguma ocorrência deste tipo, existe a possibilidade de serem violados os princípios de confidencialidade, de integridade e de disponibilidade das informações, que formam os três pilares fundamentais do conceito de segurança da informação. Isto torna a adoção de práticas de monitoramento de conexões extremamente importante para ajudar a evitar ataques externos que possam explorar vulnerabilidades existentes na rede e possam fazer com que dados armazenados em servidores sejam subtraídos ou modificados por indivíduos mal intencionados (violações de

confidencialidade e de integridade), bem como para tornar mais rápida a resolução de quedas de conexões de rede, que comprometem a disponibilidade do acesso remoto, rápido e permanente a estes dados (violação de disponibilidade).

A definição da necessidade de implantação de ferramentas de monitoramento não se baseia em números absolutos de elementos presentes na rede a ser avaliada; não existe uma quantidade mínima de estações de trabalho, de servidores ou de quaisquer outros tipos de itens de rede presentes na infraestrutura computacional da organização para que a utilização destas ferramentas seja necessária. Caberá somente à própria organização - mais especificamente, aos responsáveis por seu setor de infraestrutura - avaliar a necessidade de se efetuar esta implantação e, em caso positivo, efetuar um processo de análise das ferramentas disponíveis no mercado para definir quais delas poderão atender de forma mais satisfatória às suas necessidades, bem como para verificar o custo-benefício da aquisição de versões pagas destas ferramentas em caso de existirem funcionalidades presentes nestas que sejam interessantes à política de monitoramento a ser adotada e que não estejam presentes em suas versões disponibilizadas de forma gratuita.

Caso a estrutura computacional da organização possua pequeno porte, como, por exemplo, em organizações que utilizam a computação somente para auxílio a tarefas administrativas, muito provavelmente não haverá a necessidade de se implantar um sistema de monitoramento; porém, uma vez que vários aspectos deste tipo de tarefa dependem da utilização de conexões de Internet, é possível que isto seja considerado para que problemas de instabilidade e queda destas conexões possam ser resolvidos o mais rapidamente possível. Para este tipo de ambiente, o monitoramento, caso seja considerado necessário, tende a envolver a utilização de sistemas mais simples.

Por outro lado, organizações de médio a grande porte, especialmente as que pertencem à área de Tecnologia da Informação, tendem a possuir maior abrangência de setores com funcionários utilizando computadores, bem como uma maior quantidade de servidores que desempenham diversos serviços de suma importância, como e-mail, FTP[3], bancos de dados, serviços de diretório[4], DNS[5], firewall, proxy, virtualização e VPN. A infraestrutura

[3] File Transfer Protocol (Protocolo de Transferência de Arquivos). É o protocolo utilizado para se efetuar upload de arquivos para um servidor web.

[4] Sistemas utilizados para prover nomes de usuário e senhas para ingresso de indivíduos em uma rede e possibilitar o controle de acesso sobre conteúdos e funcionalidades desta rede, como, por exemplo, arquivos compartilhados e acesso via VPN. O serviço de diretório mais utilizado é o Active Directory, da Microsoft.

computacional destas empresas pode até mesmo estar distribuída por mais de um andar ou, em casos extremos, por mais de um edifício. Para estas organizações, a utilização de sistemas de monitoramento mais complexos e abrangentes é uma medida extremamente recomendável, senão mandatória, uma vez que o pleno funcionamento de seus processos de trabalho tende a depender de uma maior quantidade de tarefas computacionais críticas e dependentes de conexões de rede.

Além de monitorar as conexões utilizadas e o nível de tráfego de dados relativo a cada item de uma rede em que está instalado, um sistema de monitoramento possui também a capacidade de informar dados relativos à utilização de determinados componentes físicos de cada um dos servidores e de cada uma das estações de trabalho que estão presentes na rede, como, por exemplo, o nível de utilização de cada disco rígido instalado, o nível de utilização da memória RAM e o nível de temperatura da CPU. Estando de posse destas informações, os responsáveis pelo gerenciamento da rede podem proceder de forma similar a quando efetuam resoluções de problemas de utilização de conexões de rede, sendo possível, desta forma, a rápida verificação da existência de níveis indesejados de utilização dos aspectos físicos de cada máquina. Isto torna possível tomar as devidas providências para que eventuais contratempos sejam resolvidos com eficiência, impedindo, assim, a interrupção do processo de trabalho da organização por problemas envolvendo aspectos físicos em seus servidores e nas máquinas utilizadas por seus funcionários.

2.2 O protocolo SNMP

Independentemente do tamanho do cenário de infraestrutura computacional em que esteja inserido e de quantos e quais aspectos dos ativos de rede da referida infraestrutura estejam sendo ou venham a ser monitorados, um sistema de monitoramento de redes precisa, primeiramente, ser capaz de efetuar varreduras em todos os ativos da rede que estejam configurados para monitoramento, com o objetivo de extrair destes os dados de que um administrador de rede necessita. Essa tarefa fundamental é realizada através da utilização do protocolo SNMP (Simple Network Management Protocol).

---

[5] Domain Name Server (Servidor de Nome de Domínio). É o serviço que assigna nomes de domínio a endereços IP. Em redes corporativas, costuma também ser utilizado juntamente a serviços de diretório para delegar permissões individuais ou conjuntas de acesso a sites da Internet.

Segundo Mauro e Schmidt (2005), o núcleo do SNMP consiste em um conjunto de operações para obtenção de informações e das próprias informações obtidas por essas operações, que permitem ao administrador de uma rede gerenciada verificar e modificar o estado de dispositivos presentes nesta rede. O protocolo SGMP (Simple Gateway Management Protocol), antecessor do SNMP, foi desenvolvido para efetuar tarefas de gerenciamento de roteadores, mas seu sucessor, sendo um protocolo com mais funcionalidades, possibilita o gerenciamento de qualquer tipo de dispositivo com o qual possua compatibilidade, seja este um componente de hardware ou de software (servidores web e bancos de dados, por exemplo).

Oliveira (2002) fornece mais detalhes sobre a origem do gerenciamento baseado neste protocolo:

> "O embrião do gerenciamento baseado em SNMP foi a IETF (Internet Engineering Task Force), uma organização que cria padrões para a Internet. O alvo inicial foram os roteadores TCP/IP e os computadores servidores (hosts). Entretanto, a proposta de gerência baseada em SNMP é intrinsecamente genérica de forma que pode ser usada para administrar muitos tipos de sistemas. Esta proposta pode ser usada com redes de computadores, redes de tráfego automotivo, redes de controle de temperatura, redes de irrigação, etc. Assim, pode-se dizer que praticamente qualquer sistema on-line consistindo de uma coleção de dispositivos interligados por elementos de comunicação pode empregar o SNMP." (OLIVEIRA, 2002)

Como o SNMP foi projetado e oferecido rapidamente em uma época em que a necessidade de gerenciamento de rede começava a ficar premente, ele encontrou uma ampla aceitação. Hoje, esse protocolo é a estrutura de gerenciamento de rede mais amplamente usada e disseminada. (KUROSE, ROSS; 2010)

Kurose e Ross (2010), bem como Braga (2012), mostram que uma infraestrutura gerenciada pelo SNMP possui os seguintes componentes, cuja estruturação em uma rede gerenciada está esquematizada na figura 2:

a) **Entidade gerenciadora**: É o ponto central da infraestrutura de gerenciamento da rede. Consiste em uma aplicação que, após receber e processar os dados coletados pelo protocolo SNMP, disponibiliza estes dados para o administrador de rede, que é o elo humano entre a infraestrutura computacional da empresa e seus funcionários. Os softwares utilizados para este fim são chamados de sistemas de monitoramento de redes (na sigla em inglês, NMS - *Network Monitoring System)*

e são instalados em servidores dedicados, com o objetivo de estarem sempre em funcionamento utilizando o máximo de estabilidade possível.

b) **Dispositivo gerenciado**: Nome dado a cada um dos equipamentos com suporte ao SNMP que estão presentes em uma rede gerenciada. Qualquer um dos componentes físicos da rede (servidores, estações de trabalho, modems, roteadores, switches ou impressoras) pode ser um dispositivo gerenciado. Dentro de um dispositivo gerenciado há **objetos gerenciados**, que possuem os dados a serem monitorados pela entidade gerenciadora e podem ser tanto peças de hardware (uma placa de interface de rede dentro de um roteador, por exemplo) como parâmetros de software.

c) **Agente de gerenciamento**: Presente em cada um dos dispositivos gerenciados, é uma peça de software que tem a missão de recolher os dados dos objetos gerenciados presentes dentro destes dispositivos e efetuar mudanças na configuração destes objetos de acordo com solicitações efetuadas pela entidade gerenciadora.

d) **Protocolo de gerenciamento de rede**: É o dispositivo lógico de comunicação utilizado pela entidade gerenciadora e pelos dispositivos gerenciados para enviar e responder a requisições de dados e solicitações de configurações de parâmetros de objetos gerenciados. Como visto anteriormente, o SNMP atua nesta área, sendo o protocolo de maior acepção e utilização.

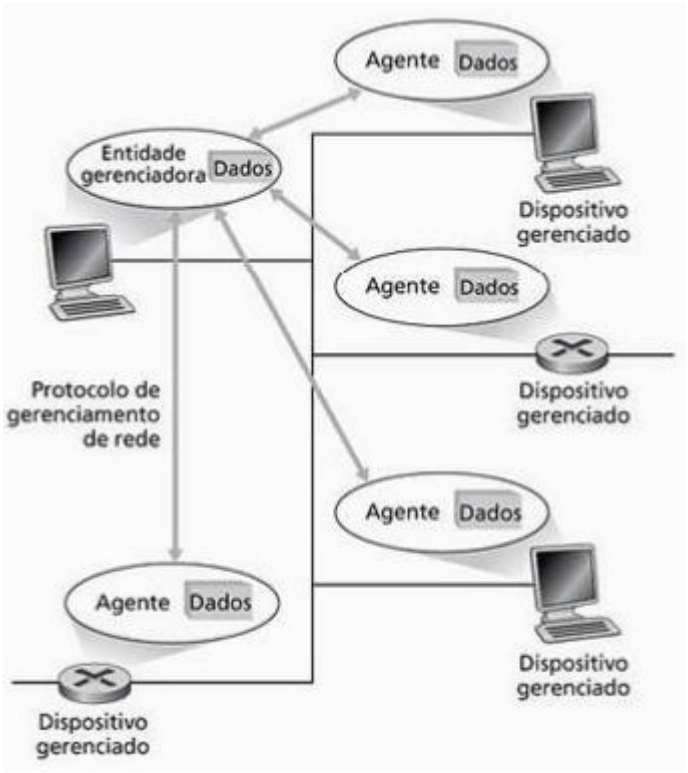

Figura 2 - Principais componentes de uma arquitetura de gerenciamento de rede. (KUROSE; ROSS, 2010)

Uma entidade gerenciadora pode enviar solicitações aos dispositivos gerenciados para requisitar os seguintes tipos de informações, segundo Microsoft (2003):

a) Identificação e estatísticas relativas ao protocolo de rede.
b) Identificação dinâmica de dispositivos ligados à rede.
c) Dados de configuração de hardware e software.
d) Estatísticas de uso e performance de dispositivos.
e) Mensagens de erro e de eventos relativas a dispositivos.
f) Estatísticas de uso de programas e aplicações.

Ainda segundo Microsoft (2003), caso a entidade gerenciadora possua permissão de escrita nos dispositivos, é possível também enviar requisições de alteração de configuração a um dispositivo, que serão executadas pelo agente de gerenciamento. Este tipo de requisição, porém, está limitado a um pequeno conjunto de parâmetros que possuem acesso de leitura e escrita predefinido; a maioria dos parâmetros aceita apenas acesso para leitura.

Os objetos gerenciados também podem fornecer dados à entidade gerenciadora sem necessidade de uma requisição prévia por parte desta. Isso é feito através de **traps**, que, de

acordo com Mauro e Schmidt (2005), são notificações assíncronas enviadas para avisar à entidade gerenciadora sobre a ocorrência de problemas em um dispositivo gerenciado. como, por exemplo, um aviso de que o limiar crítico estabelecido para uso de memória em um servidor foi atingido. Após receber uma trap, a entidade gerenciadora, através de suas possibilidades e configurações, decidirá o que fazer - ainda que a ação a ser feita seja somente enviar um e-mail com o aviso referente ao problema.

Os dados que são coletados pelo SNMP em cada um dos dispositivos gerenciados e enviados à entidade gerenciadora (sistema de monitoramento) estão localizados em uma estrutura denominada Base de Informações de Gerenciamento (na sigla em inglês, MIB - Management Information Base). O RFC[6] 1066, que explicou e definiu a base de informação necessária para monitorar e controlar redes baseadas no protocolo TCP/IP, apresentou a primeira versão da MIB, a MIB-I. O RFC 1066 foi aceito pela IAB (Internet Activities Board) como padrão no RFC 1156. O RFC 1158 propôs uma segunda MIB, a MIB-II, que expandiu a base de informações definida na MIB-I e foi aceita e formalizada como padrão no RFC 1213.[7]

Rizo (2011) explica que uma MIB possui organização em formato de árvore devido ao grande número (na casa dos milhares) de variáveis de gerência que podem ser disponibilizadas por um agente gerenciado que utilize o protocolo SNMP. Estas variáveis se encontram nas folhas da árvore da MIB e são denominadas **objetos**.

Um exemplo da esquematização em árvore da MIB-II pode ser visto na figura 3.

[6] Request for Comment (pedido para comentário). É um tipo de documento técnico desenvolvido e mantido pela IETF (Internet Engineering Task Force), uma organização destinada a criar padrões para a Internet. Cada um deles deve detalhar o funcionamento de todos os aspectos do protocolo proposto. (Fonte: https://canaltech.com.br/o-que-e/internet/O-que-e-um-RFC/)

[7] Todos os RFCs podem ser encontrados através da ferramenta de pesquisa disponível em https://tools.ietf.org/html/, bastando inserir o código do RFC que se deseja consultar.

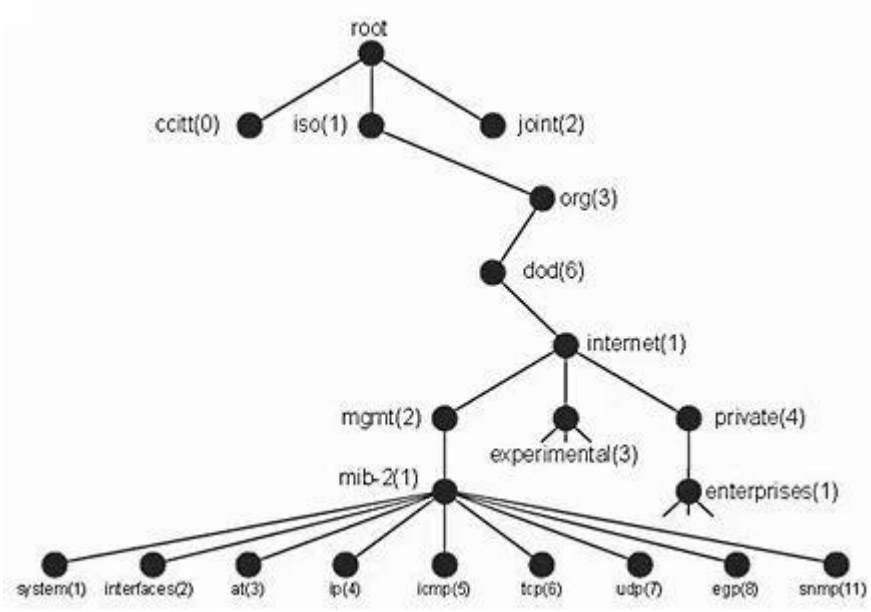

Figura 3 - Exemplo de árvore da MIB-II. (RIZO, 2011)

BRISA (1993), Rose (1995) e Microsoft (2003), bem como Fang/Leiward (1993) e Mauro/Schmidt (2005) explicam a função de cada um dos nós da árvore que compõe uma MIB:

- O nó *root*, a raiz da árvore, contém três filhos, relativos a organizações de padronização: Os nós *ccitt, iso* e *joint*. O nó *ccitt* é administrado pela organização suíça CCITT (em francês, Comité Consultatif International Téléphonique et Télégraphique), que faz parte do Setor de Padronização de Telecomunicações ITU-T (International Telecommunication Union - Telecommunication Standardization Sector). O nó *iso* é administrado pela organização ISO (International Standardization Organization). O nó *joint* é administrado conjuntamente pela CCITT e pela ISO. Destes três nós, apenas o nó *iso* é relativo ao SNMP.

- Abaixo do nó *iso* está o nó *org*, que foi definido pela ISO para conter outras organizações, sendo uma destas o Departamento de Defesa dos EUA (DOD - Department of Defence), que está presente no nó *dod*. Abaixo do nó *dod* está o nó relativo à Internet, que possui o mesmo nome (*internet*).

- O nó *internet* possui 4 subárvores. O nó *directory* (ausente da figura 3) contém informações relativas aos serviços de diretório (padrão X.500). O nó *mgmt* (de "management") contém informações de gerenciamento, sendo esta subárvore a que contém o nó *mib-2*, relativo à MIB homônima. O nó *experimental* contém os objetos que ainda estão sendo pesquisados pela IAB. O nó *private* possui a sub-árvore do nó *enterprises*, que é relativa aos objetos definidos por organizações privadas.

- Abaixo do nó *mib-2* estão os nós relativos aos objetos que fornecem informações sobre os dispositivos da rede:
    - *system*: Sistema de operação dos dispositivos da rede.
    - *interfaces*: Interfaces da rede com o meio físico.
    - *at* (*address translation*): Mapeamento (tradução) de endereços IP em endereços físicos.
    - *ip*: Protocolo IP.
    - *icmp*: Protocolo ICMP.
    - *tcp*: Protocolo TCP (transporte de pacotes segmentados).
    - *udp*: Protocolo UDP (transporte de datagramas).
    - *egp*: Protocolo EGP (roteamento de pacotes).
    - *cmot*: Protocolo CMOT.
    - *transmission*: Meios de transmissão.
    - *snmp*: Protocolo SNMP.

Cada um dos nós da árvore de uma MIB possui um número identificador. Esse número é denominado OID (Object Identifier) e sua função é substituir os nomes dos nós da árvore na hora de se referenciar um objeto ou um nó, objetivando fazer tal referência de uma forma mais simples. A subárvore relativa ao nó da MIB-II, por exemplo, pode ser referenciada como **1.3.6.1.2.1** ao invés de **iso.org.dod.internet.mgmt.mib-2**, de uma forma similar aos endereços IP.

Outro aspecto importante do SNMP é o uso de communities (comunidades), que, segundo Mauro e Schmidt (2005), "não são nada mais do que senhas; strings de texto puro que permitem que qualquer aplicativo baseado em SNMP (que reconheça a string) tenha acesso a informações de gerenciamento de um dispositivo".

2.3 Sistemas de monitoramento de redes

Como explicado no item anterior, o monitoramento de uma rede é efetuado através de aplicações que, basicamente, objetivam utilizar-se de protocolos (como, por exemplo, o SNMP) para obter informações sobre os componentes da infraestrutura. Dias (2008) mostra que estes sistemas são divididos em sistemas de acesso local e sistemas com acesso via web, bem como lista algumas diferenças entre estes dois tipos de sistemas:

a) Sistemas com acesso via web, como o exemplificado na figura 4, podem, como seu próprio nome indica, ser acessados de qualquer lugar do mundo e através de qualquer dispositivo em que seja possível utilizar os mesmos navegadores de Internet que são utilizados cotidianamente (Google Chrome, Mozilla Firefox, Opera, Safari, dentre outros), enquanto os sistemas de acesso local, por possuírem interface exibida diretamente a partir da execução do software instalado (como exemplificado na figura 5), demandam que o usuário possua acesso ao servidor onde está o sistema, o que só pode ser feito estando-se diretamente nas instalações onde o servidor se localiza ou acessando-o remotamente através de uma conexão VPN à rede da empresa ou de ferramentas de acesso remoto, como, por exemplo, TeamViewer, VNC Viewer ou Remote Desktop.

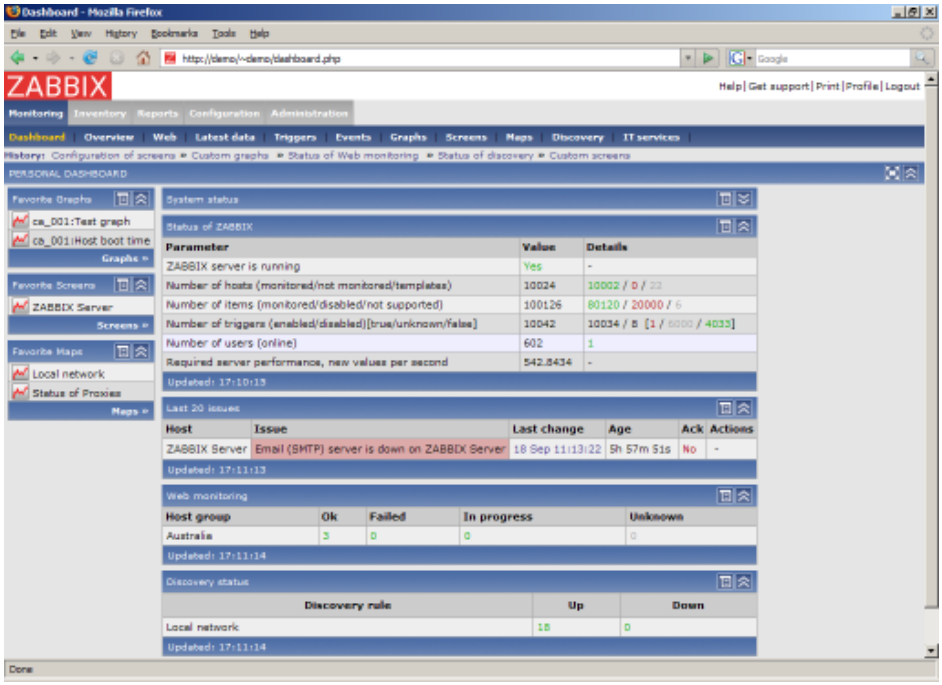

Figura 4 - Interface do Zabbix, um sistema de monitoramento com acesso web. (Disponível em http://packetlife.net/media/armory/screenshots/zabbix-130.png)

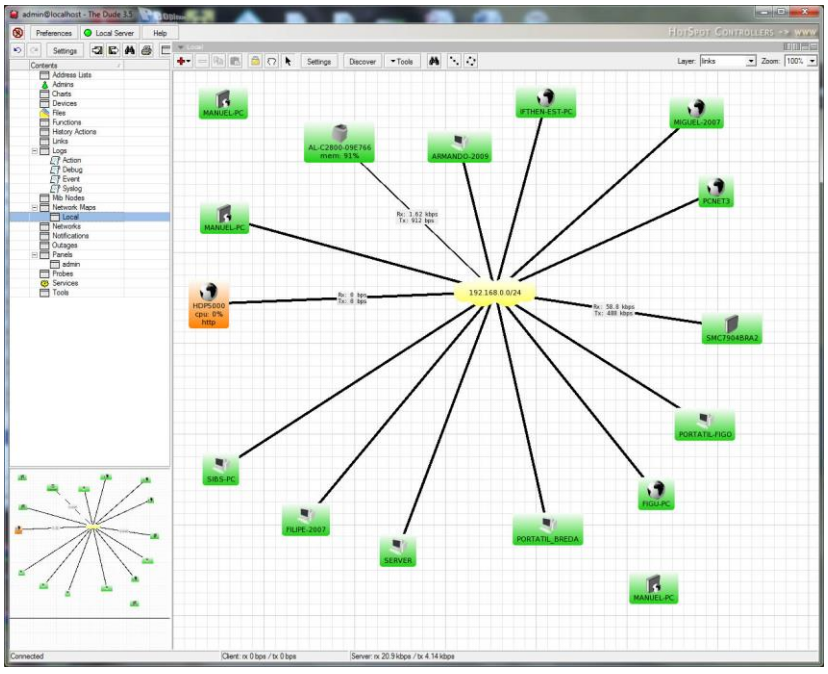

Figura 5 - Interface do The Dude, um sistema de monitoramento com acesso local. (Disponível em http://pplware.sapo.pt/wp-content/images2010/imagem_the_dude01.jpg)

b) Sistemas de acesso local não são capazes de atingir um bom nível de escalonamento para redes grandes, o que significa que, à medida que o tamanho da rede aumenta, a carga de processamento pode atingir um nível no qual não é mais possível monitorar os ativos de rede por completo. Sistemas de acesso via web também apresentam algumas limitações no que se refere à escalabilidade, mas este problema pode ser contornado efetuando-se a divisão da rede em setores independentes - o que faz com que o monitoramento passe a ser relativo a cada um destes setores, garantindo, assim, um melhor gerenciamento de redes extremamente grandes.

c) Sistemas de acesso via web geralmente possuem licenças de código livre (open-source), o que possibilita à comunidade de usuários de sistemas deste tipo colaborar com a equipe de desenvolvimento, implementando novas funcionalidades - através de mudanças no código ou da criação de plugins - e corrigindo erros que estejam presentes no código original ou mesmo em funcionalidades implementadas por outros desenvolvedores externos. Já os sistemas de monitoramento local geralmente possuem licenças proprietárias, o que cria uma barreira para a evolução destes sistemas devido ao fato de que as funções de monitoramento disponíveis são, normalmente, pré-definidas e limitadas pela equipe de desenvolvimento, o que torna impossível a terceiros terem acesso ao código de um sistema deste tipo - e, por consequência, impede a realização de esforços colaborativos que poderiam contribuir para melhorar o sistema mais rapidamente.

Dadas estas características, é possível concluir que sistemas de monitoramento com acesso local tendem a possuir maior frequência de utilização em empresas de pequeno porte e outros ambientes que não demandem a utilização de muitas funcionalidades, pois, devido a possuírem funcionamento mais limitado, tendem a demandar menos esforço para sua instalação, configuração e utilização. Por outro lado, a utilização de sistemas de monitoramento com acesso via web encontra bastante popularidade em ambientes corporativos de alto nível, devido à maior complexidade de sua infraestrutura computacional; por esse motivo, foi escolhido um sistema de monitoramento web para este trabalho, denominado Centreon, que será detalhado no próximo capítulo.

A despeito das diferenças listadas, tanto os sistemas de acesso local como os sistemas de acesso via web compartilham, além da utilização do protocolo SNMP para obter informações, uma outra característica comum e essencial a seu funcionamento básico: A capacidade de tratar as informações obtidas para que sejam exibidas de tal forma que os utilizadores do sistema possam interpretá-las apropriadamente. Isto é feito através da utilização de vários tipos de tabelas e gráficos, que, independentemente da forma como são apresentados, facilitam o correto entendimento das informações sobre os itens da rede que estão sendo monitorados e dos registros destas informações no histórico do sistema.

3 O sistema de monitoramento Centreon

Para o experimento apresentado neste trabalho, será utilizado o sistema Centreon para implantar o monitoramento da infraestrutura de rede da Escola de Informática Aplicada da UNIRIO (Universidade Federal do Estado do Rio de Janeiro), responsável pelo curso de Sistemas de Informação e uma das escolas que compõem o Centro de Ciências Exatas e Tecnologia (CCET), responsável, dentre outros, pelo curso de Bacharelado em Sistemas de Informação (BSI).

3.1. Por que o Centreon?

Birch (2016) afirma que o ano de 2004 marcou o começo do monitoramento de redes como o conhecemos hoje, com um crescimento exponencial da quantidade de opções de sistemas de monitoramento - tanto proprietários como de código aberto - e o surgimento de sistemas como o NetSaint, o OpenNMS e o SolarWinds. Desses três sistemas mencionados, o NetSaint e o OpenNMS possuem código aberto, o que colaborou bastante para que pudessem alcançar popularidade e evoluir de forma substancial ao longo dos anos, a ponto de conquistarem diversos prêmios.

O OpenNMS, cuja interface na versão mais atual pode ser vista na figura X, foi o primeiro sistema open source de monitoramento de redes a nível empresarial do mundo (como visto na figura 6, que mostra esta informação na página inicial do site do sistema em 2015), esteve entre os vencedores do prêmio Best of Open Source (BOSSIE) da revista InfoWorld em três oportunidades (2009, 2010 e 2015), além de ter vencido o prêmio Product Excellence da empresa TechTarget em 2007 (à frente do HP OpenView e do IBM Tivoli, ambos de caráter proprietário e criados por grandes corporações) e conquistado a terceira colocação no mesmo prêmio em 2009.[8] Porém, dentre os dois sistemas de código aberto mencionados, o NetSaint foi o que mais evoluiu.

[8] Mais detalhes sobre os prêmios conquistados pelo OpenNMS podem ser vistos em http://wiki.opennms.org/wiki/Awards.

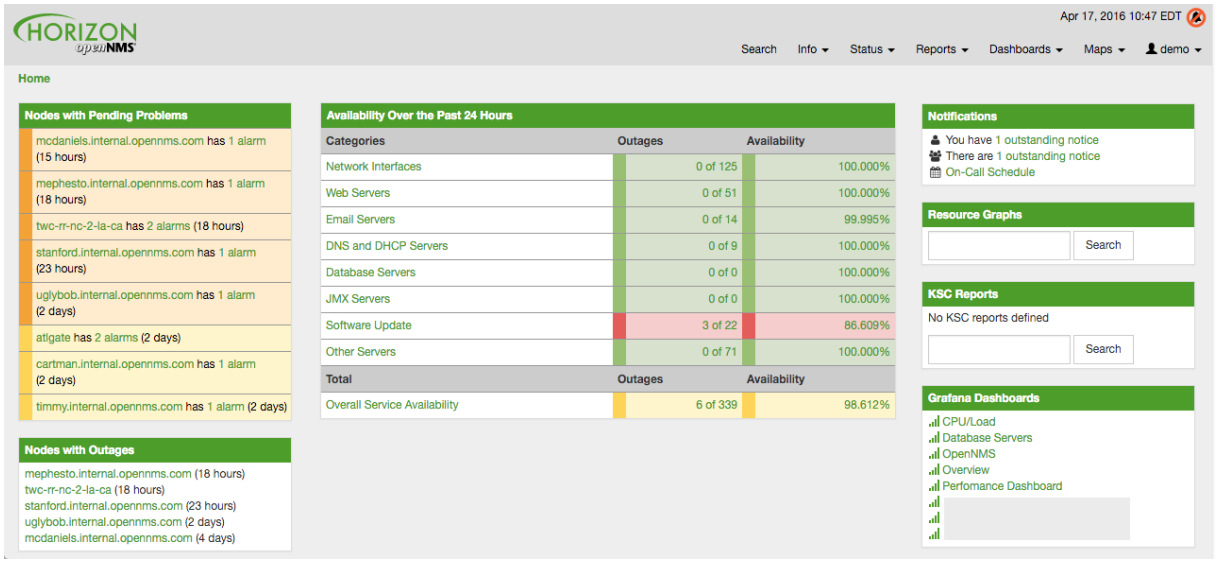

Figura 6 - Interface da versão Horizon do OpenNMS. (Disponível em https://docs.opennms.org/opennms/branches/develop/guide-admin/images/webui/startpage/01_grafana-box.png)

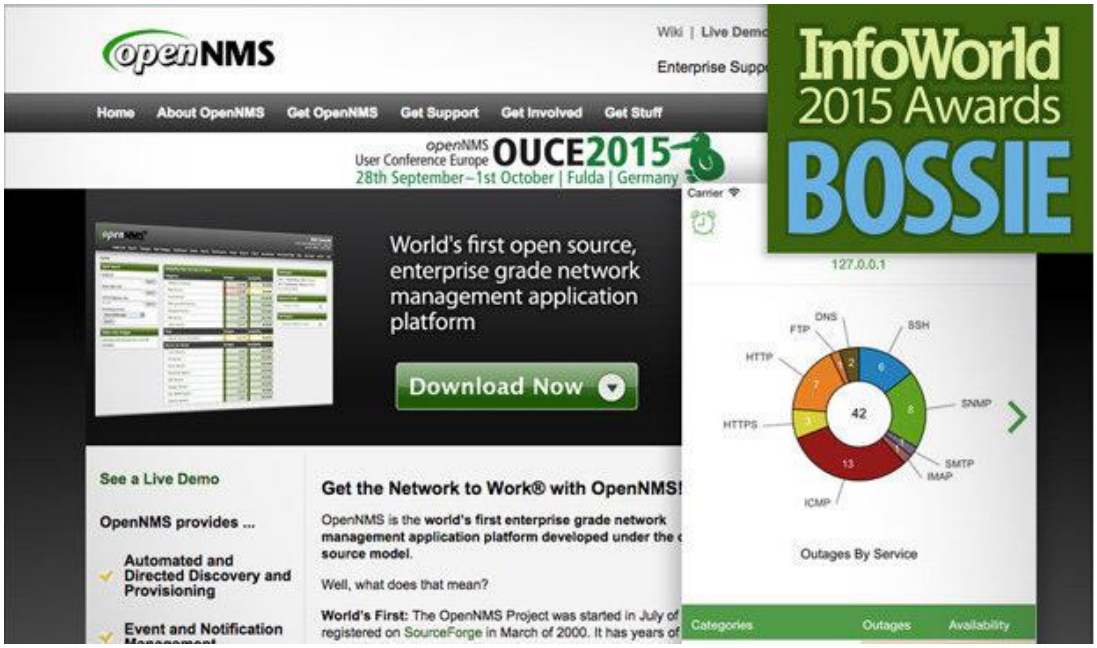

Figura 7 - Página inicial do site do OpenNMS em 2015, quando foi um dos vencedores do BOSSIE Awards da revista InfoWorld. (Disponível em http://www.infoworld.com/article/2982962/open-source-tools/bossie-awards-2015-the-best-open-source-networking-and-security-software.html#slide4)

Figura 8 - Exemplo de interface do NetSaint. (Disponível em http://www.soi.wide.ad.jp/class/20010011/slides/11/img/14.png)

Em sua primeira versão, muito antes de possuir esse nome, o NetSaint era constituído basicamente por uma ferramenta que, através de aplicações de terceiros, efetuava ping para servidores NetWare da Novell - onde seu criador, Ethan Galstad, trabalhava - e enviava páginas numéricas. Em 1998, dois anos após o surgimento da primeira versão, Galstad, interessado em entrar no ramo de ferramentas de monitoramento, utilizou as idéias já estabelecidas para construir um novo sistema, que seria lançado no ano seguinte, já sob o nome NetSaint.

Em 2002, por problemas de registro de marca, Ethan mudou o nome do NetSaint para Nagios, um acrônimo recursivo para “Nagios Ain’t Gonna Insist on Sainthood” - em referência ao abandono do nome original do sistema. A mudança de nome não impediu o sistema de continuar evoluindo, e, em junho de 2005, o Nagios ganhou seu primeiro prêmio, sendo eleito Projeto do Mês pelo site SourceForge.net.

Nos anos seguintes, o Nagios continuou obtendo prêmios e reconhecimentos. Em 2006, no ano seguinte a seu primeiro prêmio, foi classificado como “ferramenta essencial” pelo site eWeek. Em 2007, teve um de seus anos mais gloriosos: Foi finalista da categoria “Melhor Ferramenta ou Utilitário para SysAdmins” do prêmio SourceForge.net Community Choice Awards, eleito um dos mais importantes softwares open source de todos os tempos

pelo site eWeek, classificado como uma das 5 melhores ferramentas open source de segurança para ambientes corporativos pelo site LinuxWorld.com e eleito Ferramenta de Monitoramento do Ano pelo site LinuxQuestions.org. Ainda em 2007, o Nagios deu um passo importante para seu crescimento: Se tornou uma empresa após Galstad fundar a Nagios Enterprises com o objetivo de fornecer serviços de desenvolvimento e consultoria relativos a sua criação.

Os anos subsequentes foram marcados por cada vez mais prêmios e reconhecimentos[9], fazendo com que a Nagios Enterprises pudesse crescer substancialmente e evoluir seu produto para um alto padrão. Nos dias de hoje, o Nagios possui um enorme alcance entre grandes corporações, tendo como seus clientes algumas das gigantes de diversas áreas, como AOL, Domino's Pizza, AT&T, Linksys, L'Óreal, Philips, Sony, Toshiba e Universal[10].

Nenhum sistema é perfeito, porém, e com o Nagios não foi diferente. Uma das principais críticas ao sistema ao longo dos anos residia na falta de possibilidade de configurar o sistema através de sua interface web, o que fazia com que fosse necessário ter acesso direto ao servidor para aplicar configurações diretamente nos arquivos do sistema e levou ao surgimento de várias aplicações de frontend para o Nagios[11], que, apesar de diferentes entre si, possuíam o objetivo comum de facilitar o trabalho do administrador do sistema em relação às etapas de configuração e fornecer uma interface melhor - o que é outro problema do Nagios, cuja interface praticamente não mudou desde os tempos de NetSaint e é considerada pouco intuitiva e básica demais por boa parte de seus usuários. Há também a ausência de geração nativa de gráficos, o que torna necessária a utilização de ferramentas criadas por terceiros.

[9] Mais detalhes sobre os prêmios conquistados pelo Nagios podem ser vistos em https://www.nagios.com/awards/.

[10] Uma lista mais abrangente de grandes corporações que utilizam o Nagios pode ser encontrada em http://www.nagios.com/users/.

[11] Alguns exemplos de aplicações de frontend desenvolvidas para o Nagios são descritos em http://www.ducea.com/2008/01/16/10-nagios-web-frontends/.

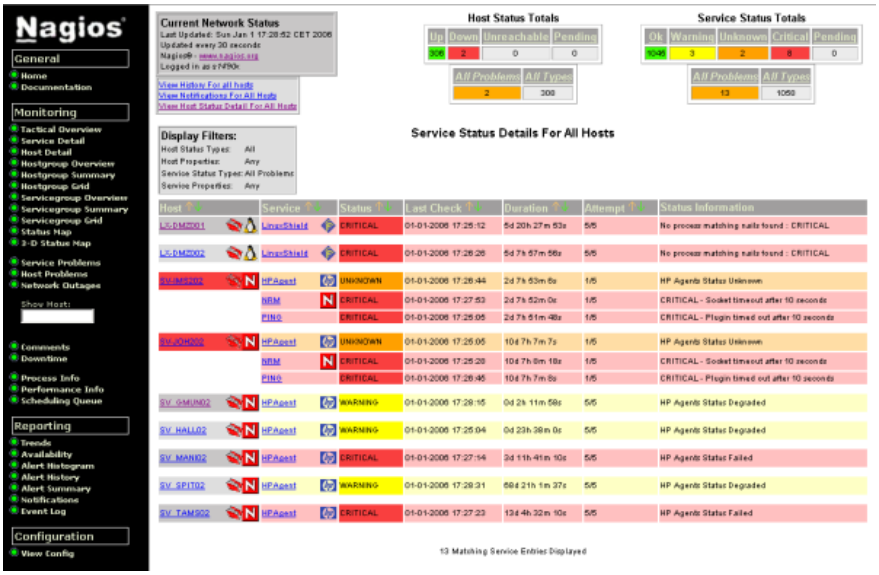

Figura 9 – Exemplo de interface do Nagios em uma versão antiga do sistema. (Disponível em https://www.novell.com/coolsolutions/img/nagios_html_2f522541.png)

Foi pensando nestes problemas que uma das aplicações de frontend disponíveis para o Nagios evoluiu a ponto de se tornar um sistema de monitoramento independente, que utiliza os mesmos princípios do Nagios e é compatível com suas funcionalidades (além de adicionar novas), mas não precisa de uma instalação do Nagios em si para funcionar, ao contrário de um frontend comum. Essa aplicação, mostrada na figura 10, é o Centreon, criado pela companhia francesa Merethis.

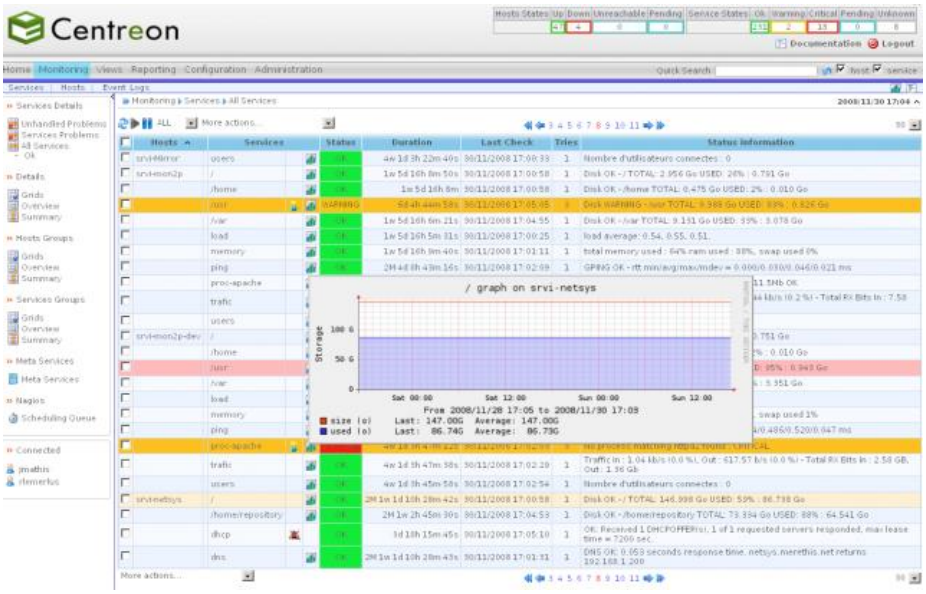

Figura 10 - Exemplo de interface do Centreon em uma versão antiga do sistema. (Disponível em http://shinken.readthedocs.io/en/latest/_images/centreon.png)

Como relatado anteriormente, o Nagios conseguiu, apesar dos problemas mencionados, obter um quinhão bastante significativo do uso de sistemas de monitoramento em grandes corporações. Tal comprovação de qualidade, conjuntamente ao fato de o Centreon, mesmo depois de se tornar independente do Nagios, ter continuado a utilizar os princípios deste como base de funcionamento e de melhorias, fez com que o Centreon fosse o sistema escolhido para este experimento. Outro fator que influenciou na decisão foi a pouca quantidade de publicações em português sobre o sistema.

Mais detalhes sobre o Centreon serão informados no próximo capítulo, onde serão mostrados seu processo de instalação na rede UNIRIOTEC, pertencente ao CCET da UNIRIO, e vários aspectos da interface do sistema e de seu funcionamento.

4 O Centreon na Escola de Informática Aplicada da UNIRIO

O Centro de Ciências Exatas e Tecnologia da UNIRIO, localizado no Campus Praia Vermelha, no bairro da Urca, na Zona Sul da cidade do Rio de Janeiro, foi fundado no ano de 2000 para abrigar o curso de Sistemas de Informação, que marcou seu lugar na história da universidade como seu primeiro curso de ciências exatas, sendo também o primeiro desta modalidade de cursos superiores de Tecnologia da Informação entre as universidades da cidade do Rio de Janeiro; até então, a área de TI se fazia presente nas universidades públicas cariocas somente através do curso de Ciência da Computação na Universidade do Estado do Rio de Janeiro (UERJ) e dos cursos de Ciência da Computação e Engenharia da Computação na Universidade Federal do Rio de Janeiro (UFRJ).

O prédio principal do CCET é utilizado também pelo Instituto de Biociências (IBIO), que possui dois laboratórios e dependências administrativas e de docentes em dois de seus quatro andares e com o qual divide salas de aula em um dos outros andares. Apesar de ter passado por mudanças estruturais profundas nas décadas de 2000 e 2010 com a construção de dois prédios anexos para expansão de sua quantidade de salas de aula e de suas dependências administrativas e de docentes, bem como a construção de dois auditórios (sendo um de uso exclusivo do curso de Sistemas de Informação e outro, maior, para uso também por outros cursos do Centro), sua infraestrutura - ao menos em termos de servidores e de bancos de dados - não aumentou na mesma proporção; desde a fundação do curso, praticamente toda sua estrutura computacional está localizada no andar térreo do Centro.

O CCET possui quatro principais setores em sua organização de infraestrutura, que concentram a maior parte das máquinas (servidores e computadores de uso geral) que utilizam seus recursos de rede: Uma sala de servidores, onde estão localizados os servidores de dados e fornecedores de serviços, e três Laboratórios de Informática, onde são ministradas aulas práticas de disciplinas que utilizam recursos computacionais (ambientes de programação, bancos de dados, conteúdos disponíveis via web, dentre outros). Além dos referidos setores, o CCET possui também uma Sala de Estudos com computadores de uso geral dos alunos, salas de professores (incluídas nestas as salas da Diretoria e do Decanato) com computadores de uso pessoal dos docentes, uma Secretaria com computadores de uso dos técnicos

administrativos e a sala do Diretório Acadêmico, que possui um computador para uso de seus membros e, caso esteja disponível, de outros alunos que o estejam visitando.

Para este trabalho, serão monitorados cinco servidores:

a) Servidor do Moodle[12]
b) Servidor de testes do Moodle
c) Servidor do SAT (sistema de abertura de chamados)
d) Servidor de hospedagem do portal do BSI
e) Servidor de backups

Mais detalhes sobre eles serão fornecidos em uma das próximas seções deste capítulo, que explicará como estes servidores serão inseridos no Centreon para serem monitorados.

4.1. Instalação e configuração do Centreon

A instalação do Centreon pode ser efetuada utilizando-se dois tipos de procedimentos. Caso o servidor onde a instalação será feita já possua como sistema operacional a distribuição Linux desejada para receber o Centreon, o processo será feito através do gerenciador de pacotes do Linux, que é capaz de efetuar tanto o download quanto a instalação do pacote do Centreon, sendo estes procedimentos executados automaticamente e em sequência caso o usuário utilize o parâmetro de confirmação automática da instalação do pacote do qual foi efetuado o download. Se o servidor que receberá o Centreon não possuir nenhum sistema operacional, possuir um sistema operacional que não seja uma distribuição Linux ou possuir uma distribuição Linux que não seja a desejada, é possível efetuar, no site dos fabricantes do Centreon, o download da imagem do Centreon Enterprise Server, que consiste em uma versão da distribuição CentOS exatamente igual à original, mas com o Centreon previamente instalado e pronto para ser configurado.

A versão do sistema a ser instalada será a versão 2.6.4. Para este trabalho foi preciso escolher uma versão que não é a mais atual; porém, a versão que será utilizada atende satisfatoriamente aos requisitos necessários. Como o site do Centreon atualmente não possui

[12] Sistema colaborativo destinado a unificar a disponibilização de conteúdo para alunos por parte de professores. Mais informações sobre este sistema podem ser obtidas em seu site: http://moodle.org/.

esta versão disponível para download do arquivo de imagem do Centreon Enterprise Server, o processo de instalação, demonstrado abaixo, envolverá os dois procedimentos descritos no primeiro parágrafo deste item; Será efetuada a instalação do Centreon Enterprise Server, em sua versão 3.2, disponível para download no site do Centreon, em um servidor dedicado e, após, será efetuado o downgrade para a versão 2.6.4 através do uso de pacotes.

4.1.1. Instalação do Centreon Enterprise Server 3.2

a) Acessar a seção de downloads do site do Centreon e efetuar o download da imagem ISO da versão 3.2 do Centreon Enterprise Server.

b) Iniciar o servidor com a imagem baixada (seja em DVD ou pen drive de boot no caso de um servidor físico ou com a imagem no drive virtual do software de virtualização no caso de um servidor virtual) e seguir o assistente de instalação do CentOS como seria feito em um Linux comum – até ser alcançada a etapa mostrada na figura 11, quando deve-se escolher a opção *Central server with database* para que o banco de dados do Centreon seja instalado no mesmo servidor que o sistema em si. Esta opção já vem selecionada por padrão, bastando clicar em *Next* para avançar à próxima etapa.

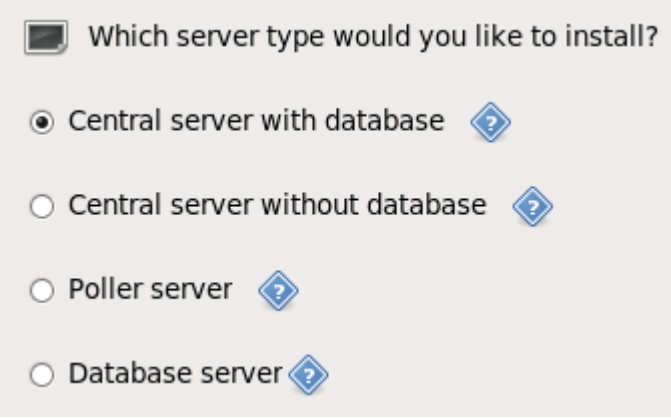

Figura 11 - Tela do assistente de instalação do Centreon Enterprise Server em que se escolhe o tipo de servidor Centreon desejado

c) Após a instalação do CentOS, acessar o URL http://[IP do servidor]/centreon. Para este trabalho, foi utilizado um servidor com este endereço já redirecionado para o endereço *http://monitor.uniriotec.br*. Se tudo estiver correto, clicar no botão *Next* na

primeira tela do assistente de instalação do Centreon, indicada na figura 12.

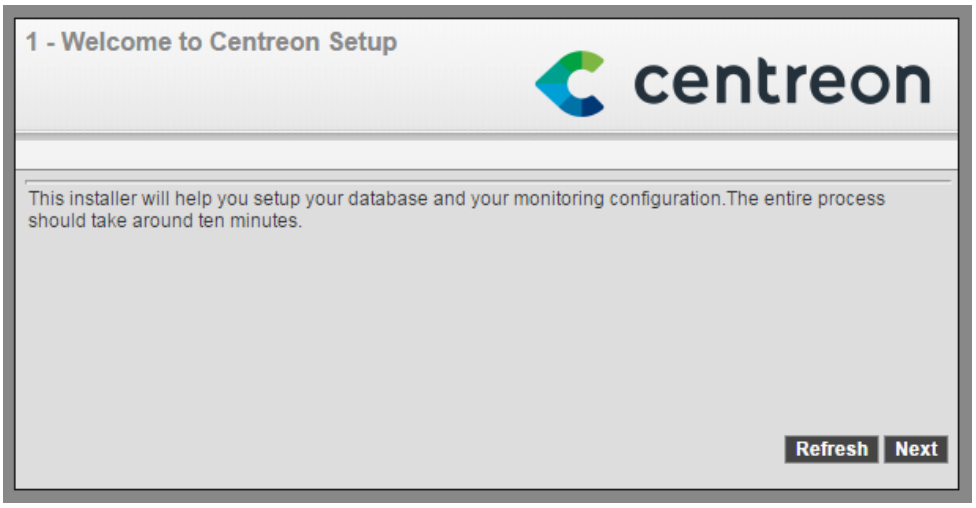

Figura 12 – Primeira tela da instalação do Centreon (*Welcome to Centreon Setup*)

d) Na tela *Dependency check up*, mostrada na figura 13, o assistente irá detectar se os módulos de dependência do Centreon estão em funcionamento. Caso todos estejam funcionando, clicar no botão *Next*, que ficará habilitado.

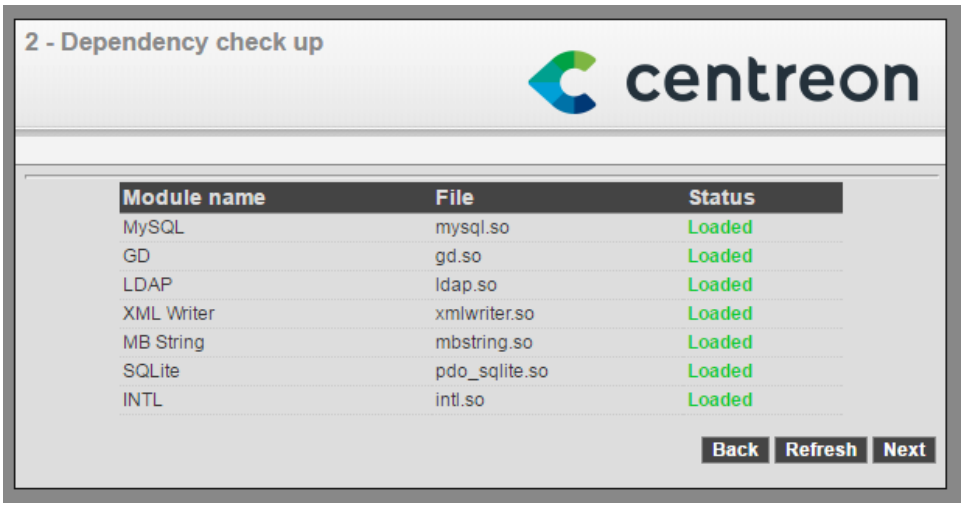

Figura 13 – Segunda tela da instalação do Centreon (*Dependency check up*)

e) Na tela *Monitoring engine information*, mostrada na figura 14, escolher o item *centreon-engine* no campo *Monitoring engine*. Todos os outros campos serão preenchidos automaticamente, exceto o último (*Embedded Perl initialisation file*), que não é necessário no momento e, por isso, pode ficar em branco. Clicar no botão *Next*.

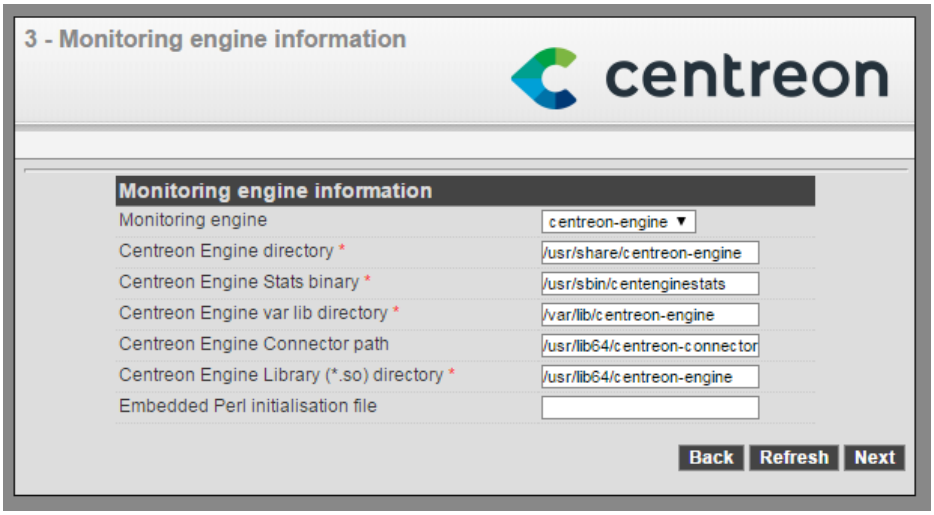

Figura 14 – Terceira tela da instalação do Centreon (*Monitoring engine information*)

f) Na tela *Broker module information*, mostrada na figura 15, escolher o item *centreon-broker* no campo *Broker Module*. Todos os outros campos serão preenchidos automaticamente. Clicar no botão *Next*.

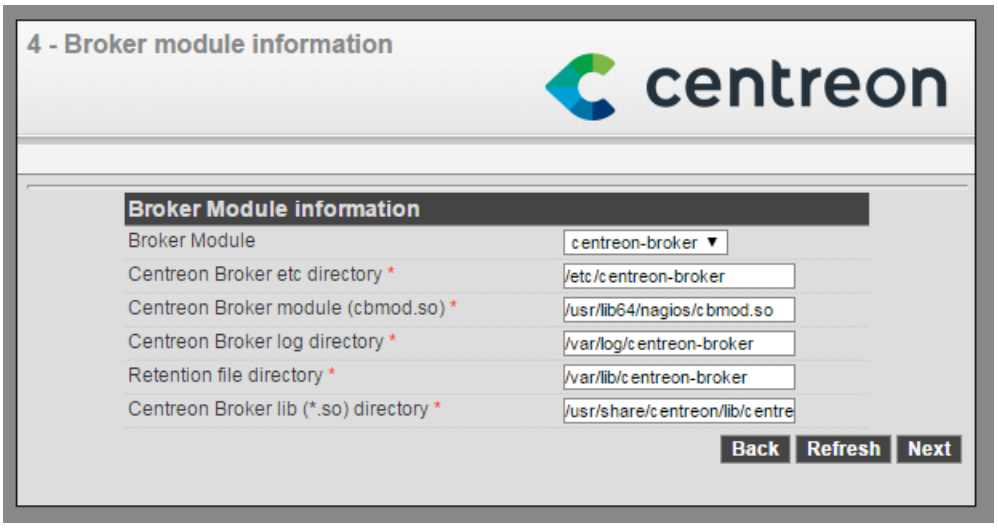

Figura 15 – Quarta tela da instalação do Centreon (*Broker module information*)

g) Na tela *Admin information*, mostrada na figura 16, será configurado o usuário de administrador padrão do Centreon. O nome de usuário (admin), presente no campo Login por padrão, é imutável, sendo preciso preencher os campos de senha, confirmação de senha, primeiro nome, último nome e endereço de e-mail. Após preencher todos os campos, clicar no botão *Next*.

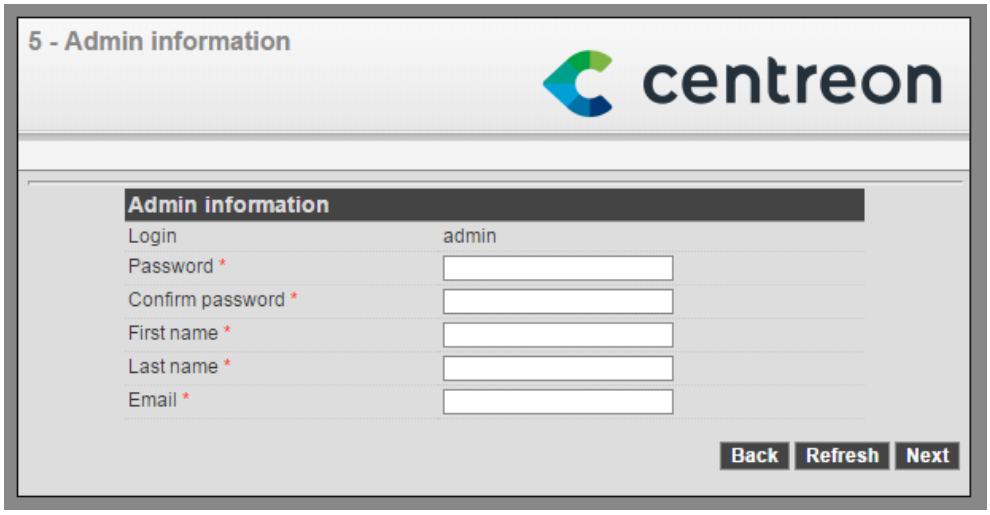

Figura 16 – Quinta tela da instalação do Centreon (*Admin information*)

h) Na tela *Database information*, mostrada na figura 17, serão configurados os dados de acesso ao banco de dados do Centreon. O campo *Database Host Address*, que indica o endereço do banco de dados, deverá ser deixado em branco para que seja indicado que o endereço é o próprio servidor local (localhost). Os campos relativos ao nome do banco de configuração (configuration database), ao nome do banco de armazenamento (storage database) e ao nome do banco de utilitários (utils database) já estão definidos por padrão, sendo necessário mudá-los somente caso desejado - o que não é recomendável, por motivos de referências em materiais externos. Definir uma senha de root para o banco no campo *Root password* não é obrigatório, mas, por motivos de segurança, é recomendável que seja feito. A senha do usuário comum padrão do banco, que é obrigatória e deve ser confirmada no campo imediatamente abaixo. Após preencher todos os campos obrigatórios, clicar em *Next*.

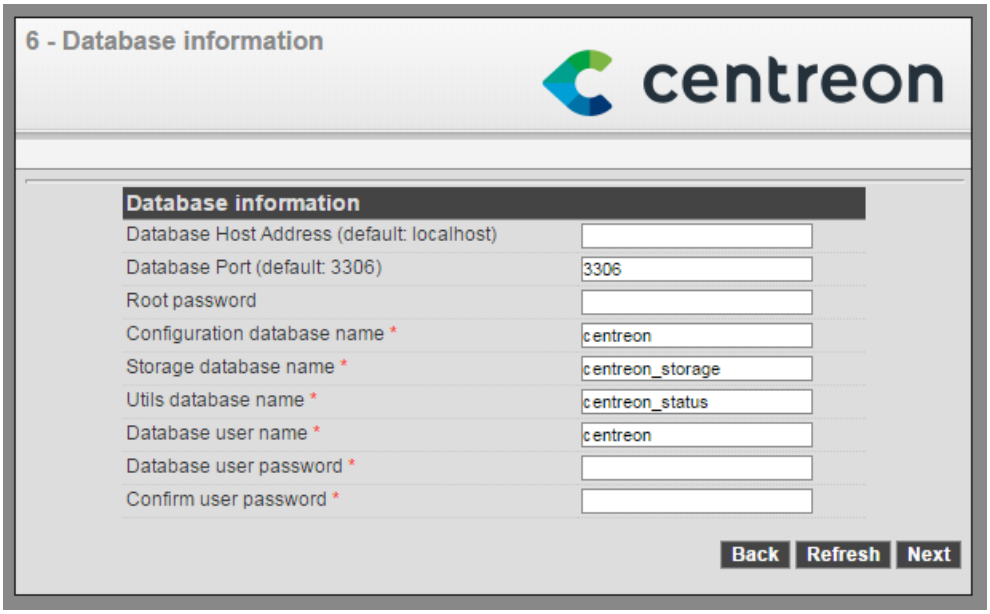

Figura 17 – Sexta tela da instalação do Centreon (*Database information*)

i) A tela *Installation*, mostrada na figura 18, indica que o Centreon está sendo instalado. Após todas as etapas (banco de configuração, banco de armazenamento, criação do usuário do banco, configuração básica e arquivo de configuração) serem concluídos, clicar em *Next*.

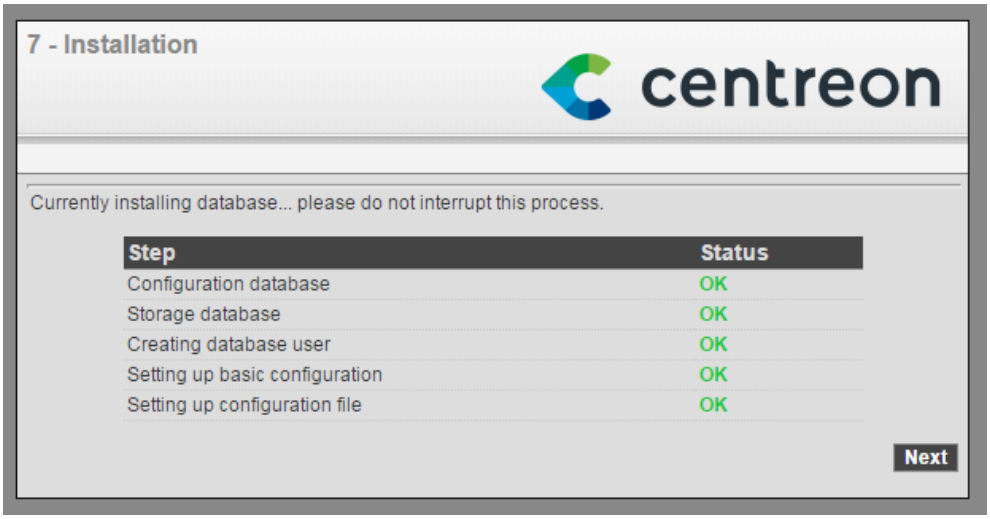

Figura 18 – Sétima tela da instalação do Centreon (*Database information*)

j) A tela *Installation finished*, mostrada na figura 19, indica que a instalação foi finalizada e lista alguns links que podem ser úteis para os usuários do Centreon: O site oficial, o fórum oficial, a documentação e o bug tracker no GitHub. Clicar no botão *Finish* para concluir a instalação.

Figura 19 – Oitava tela da instalação do Centreon (*Database information*)

4.1.2. Configuração de hostname do servidor Linux

Antes de se prosseguir, é preciso efetuar algumas configurações primárias no sistema operacional. O passo-a-passo, feito segundo Ribeiro (2015), segue abaixo:

a) Abrir o arquivo */etc/sysconfig/network* e deixá-lo como no exemplo abaixo:

NETWORKING=yes
HOSTNAME=monitor.uniriotec.br

b) Abrir o arquivo */etc/selinux/config* e deixar o parâmetro *SELINUX* como *disabled.*

c) Abrir o arquivo */etc/hosts* e deixar a linha referente ao endereço IP 172.0.0.1 da seguinte forma:

127.0.0.1 monitor.uniriotec.br monitor localhost

d) Reiniciar o servidor.

4.1.3. Downgrade para a versão 2.6.4 do Centreon

Após o servidor ser reiniciado, o downgrade para a versão 2.6.4 pode ser realizado. O passo-a-passo, feito segundo Ribeiro (2015), segue abaixo:

a) Acessar o servidor como um usuário com permissão de superusuário (root).

b) Executar os comandos abaixo, que desinstalam os bancos de dados da versão do Centreon atualmente instalada.

```
mysql -e 'drop database centreon;'
mysql -e 'drop database centreon_storage;'
mysql -e 'drop database centreon_status;'
```

c) Executar o comando abaixo, que desinstala os pacotes do Centreon da versão atualmente instalada.

```
yum remove -y \
centreon-web \
centreon-common \
centreon-broker \
centreon-broker-cbd \
centreon-engine \
centreon-connector-ssh |
centreon-broker-cbmod \
centreon-engine-extcommands \
centreon-connector-perl \
centreon-broker-core \
centreon-engine-daemon \
centreon-connector \
centreon-broker-storage \
centreon-clib
```

d) Executar o comando abaixo, que nstala os pacotes da versão 2.6.4 do Centreon.

yum install -y \
centreon-broker-storage-2.10.1-6.el6.x86_64 \
centreon-plugins-2.6.4-2.el6.noarch \
centreon-engine-daemon-1.4.15-6.el6.x86_64 \
centreon-plugin-meta-2.6.4-2.el6.noarch \
centreon-connector-1.1.2-1.el6.x86_64 centreon-trap-2.6.4-2.el6.noarch \
centreon-broker-2.10.1-6.el6.x86_64 \
centreon-broker-cbd-2.10.1-6.el6.x86_64 \
centreon-2.6.4-2.el6.noarch \
centreon-clib-1.4.2-1.el6.x86_64 \
centreon-broker-cbmod-2.10.1-6.el6.x86_64 \
centreon-engine-1.4.15-6.el6.x86_64 \
centreon-base-config-centreon-engine-2.6.4-2.el6.noarch \
centreon-connector-ssh-1.1.2-1.el6.x86_64 \
centreon-common-2.6.4-2.el6.noarch \
centreon-broker-core-2.10.1-6.el6.x86_64 \
centreon-engine-extcommands-1.4.15-6.el6.x86_64 \
centreon-web-2.6.4-2.el6.noarch \
centreon-connector-perl-1.1.2-1.el6.x86_64 \
centreon-perl-libs-2.6.4-2.el6.noarch

e) Repetir o procedimento de instalação do Centreon demonstrado no item 4.1.1, a partir do passo C.

f) A tela de login da versão 2.6.4, mostrada na figura 20, aparecerá.

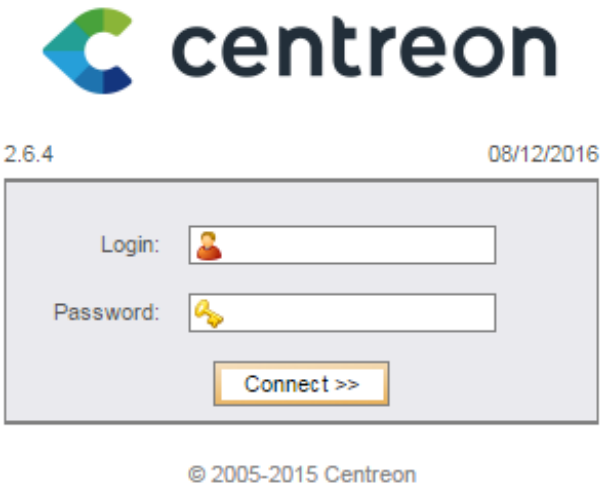

Figura 20 – Tela de login da versão 2.6.4 do Centreon.

4.1.4. Configuração do protocolo SNMP nos hosts a serem monitorados

Antes de se iniciar a etapa de configuração de hosts (os dispositivos de rede gerenciados) e de serviços (aspectos dos dispositivos gerenciados que serão disponibilizados ao Centreon, a entidade gerenciadora do presente cenário), é preciso efetuar a configuração do protocolo SNMP em cada um dos hosts a serem monitorados.
O procedimento abaixo, feito segundo Ribeiro (2015), se refere a máquinas com Linux.

a) Instalar os pacotes *net-snmp* e *net-snmp-utils* (o comando é diferente para cada distribuição Linux devido à não-padronização de uso de gerenciadores de pacotes, possuindo cada uma um gerenciador diferente)

b) Renomear o arquivo */etc/snmp/snmpd.conf* para *snmpd.conf.old* e criar um novo arquivo snmpd.conf na mesma pasta, com o seguinte conteúdo:

com2sec ConfigUser default UNIRIOTEC
com2sec ConfigUser localhost UNIRIOTEC
com2sec ConfigUser 10.0.21.29 UNIRIOTEC
group ConfigGroup v1 ConfigUser
group ConfigGroup v2c ConfigUser
view systemview included .1 80

access ConfigGroup "" any noauth exact systemview none none
syslocation "CPD-UNIRIOTEC"
syscontact "Monitor UNIRIOTEC <monitor.uniriotec@gmail.com>"
dontLogTCPWrappersConnects yes

c) Habilitar o serviço SNMP para iniciar automaticamente caso o servidor precise ser reiniciado.

chkconfig snmpd on

d) Caso o firewall esteja habilitado, liberar a porta 161 do protocolo UDP.

e) Iniciar o serviço do SNMP.

service snmpd start

f) Para testar o funcionamento do SNMP, acessar o servidor de monitoramento com um usuário que tenha permissão de superusuário (root) e utilizar o comando *snmpwalk.*

snmpwalk -v2c -c UNIRIOTEC [IP do servidor]

Se o SNMP estiver funcionando, a saída deste comando será parecida com o que é mostrado na figura 21.

```
DISMAN-EVENT-MIB::mteEventNotificationObjectsOwner."_snmpd".'_mteTriggerFired' =
 STRING: _snmpd
DISMAN-EVENT-MIB::mteEventNotificationObjectsOwner."_snmpd".'_mteTriggerRising'
= STRING: _snmpd
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd".'_linkDown' = STRING: _li
nkUpDown
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd".'_linkUp' = STRING: _link
UpDown
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd".'_mteTriggerFailure' = ST
RING: _triggerFail
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd".'_mteTriggerFalling' = ST
RING: _triggerFire
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd".'_mteTriggerFired' = STRI
NG: _triggerFire
DISMAN-EVENT-MIB::mteEventNotificationObjects."_snmpd".'_mteTriggerRising' = STR
ING: _triggerFire
NOTIFICATION-LOG-MIB::nlmConfigGlobalEntryLimit.0 = Gauge32: 1000
NOTIFICATION-LOG-MIB::nlmConfigGlobalAgeOut.0 = Gauge32: 1440 minutes
NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsLogged.0 = Counter32: 0 notific
ations
NOTIFICATION-LOG-MIB::nlmStatsGlobalNotificationsBumped.0 = Counter32: 0 notific
ations
[root@monitor ~]#
```

Figura 21 – Exemplo de saída correta do comando *snmpwalk*.

4.1.5. Configuração do Postfix

O Postfix é a aplicação que permite ao Centreon enviar e-mails - no caso, os e-mails de alertas quando algum host configurado ou serviço tem seu status modificado. Abaixo estão os passos para configurar o envio de e-mails utilizando uma conta do Gmail, que pode ser pertencente ao Gmail em si ou a qualquer domínio de e-mail cadastrado no GSuite (antigo Google Apps).

Primeiramente, é preciso habilitar o acesso a aplicativos menos seguros na conta do Gmail escolhida[13]. Após isso ser feito, deve-se seguir os seguintes passos, segundo Ribeiro (2015):

a) Acessar o servidor de monitoramento como um usuário com permissão de superusuário (root).

b) Instalar os pacotes *cyrus-sasl-plain* e *mail*.

yum install -y cyrus-sasl-plain mail

c) Editar o arquivo */etc/postfix/sasl_passwd* e adicionar a seguinte linha:

[13] Passo-a-passo disponível em https://support.google.com/accounts/answer/6010255?hl=pt-BR.

smtp.gmail.com usuárioGmail:senhaGmail

O usuário precisa ser o endereço de e-mail completo (usuário@gmail.com).

d) Mudar o usuário dono do arquivo */etc/postfix* para o usuário *postfix*

chown postfix /etc/postfix

e) Assignar o arquivo onde estão configurados o usuário e a senha do Gmail ao serviço postmap, que é a tabela de consulta do postfix.

postmap hash:/etc/postfix/sasl_passwd

f) Editar o arquivo */etc/postfix/main.cf* e deixá-lo da seguinte forma:

relayhost = smtp.gmail.com:587
smtp_tls_security_level = secure
smtp_tls_mandatory_protocols = TLSv1
smtp_tls_mandatory_ciphers = high
smtp_tls_secure_cert_match = nexthop
smtp_tls_CAfile = /etc/pki/tls/certs/ca-bundle.crt
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous

g) Habilitar o Postfix para iniciar automaticamente caso o servidor precise ser reiniciado.

chkconfig postfix on

h) Reiniciar o Postfix.

service postfix restart

i) Para testar o envio de e-mails:

echo "Teste e-mail" | mail -s "Este é um teste" EmailDestinatário

O texto após o comando *echo* indica o corpo da mensagem do e-mail e o parâmetro *-s* indica o título (subject) do e-mail.

Para verificar se o e-mail foi enviado pelo serviço, usar o seguinte comando:

tail -f /var/log/maillog

O arquivo */var/log/maillog* armazena os registros de e-mails enviados e o comando *tail*, utilizado com o parâmetro *–f*, exibe as últimas linhas de um arquivo de texto e atualiza a visualização em tempo real caso sejam feitas alterações no arquivo por outros meios.

Se o conteúdo da visualização for equivalente ao que é mostrado na figura 22, o e-mail foi enviado corretamente pelo sistema. Um exemplo de e-mail enviado como teste é mostrado na figura 22.

```
Dec  9 04:56:58 monitor postfix/pickup[21916]: E0C45BFF7C: uid=0 from=<root>
Dec  9 04:56:58 monitor postfix/cleanup[23870]: E0C45BFF7C: message-id=<20161209
065658.E0C45BFF7C@monitor.unirietec.br>
Dec  9 04:56:58 monitor postfix/qmgr[2352]: E0C45BFF7C: from=<root@monitor.uniri
otec.br>, size=480, nrcpt=1 (queue active)
Dec  9 04:57:03 monitor postfix/smtp[23872]: E0C45BFF7C: to=<calil.bfr@gmail.com
>, relay=smtp.gmail.com[64.233.186.108]:587, delay=4.4, delays=0.05/0.14/3.1/1.1
, dsn=2.0.0, status=sent (250 2.0.0 OK 1481266623 d78sm19238311qkg.49 - gsmtp)
Dec  9 04:57:03 monitor postfix/qmgr[2352]: E0C45BFF7C: removed
```

Figura 22 – Exemplo de registro de envio correto de e-mail pelo Postfix no arquivo */var/log/maillog*.

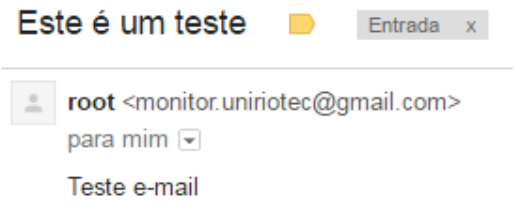

Figura 23 – Exemplo de e-mail enviado corretamente pelo Postfix.

4.2. Utilização do Centreon

Para começar a utilizar o Centreon após a instalação, é preciso efetuar login com o usuário de administrador (*admin*) utilizando a senha definida no ato da instalação do sistema. Depois disso, será preciso configurar os hosts a serem monitorados e seus respectivos serviços.

Um host é qualquer dispositivo gerenciado da rede que possa ser monitorado pelo Centreon. O monitoramento de um host no Centreon nada mais é que o conjunto de serviços configurados para este host; serviços são configurações de comandos de checagem relativos aos componentes do dispositivo que possam ter suas informações coletadas por seu agente de gerenciamento e enviadas ao Centreon, que é a entidade gerenciadora do cenário.

4.2.1. Interface principal

Ao se efetuar o login no Centreon pela primeira vez, pode ser vista a tela inicial do sistema, mostrada na figura 24. Ela possui dois itens de mais destaque: O menu principal e a barra superior.

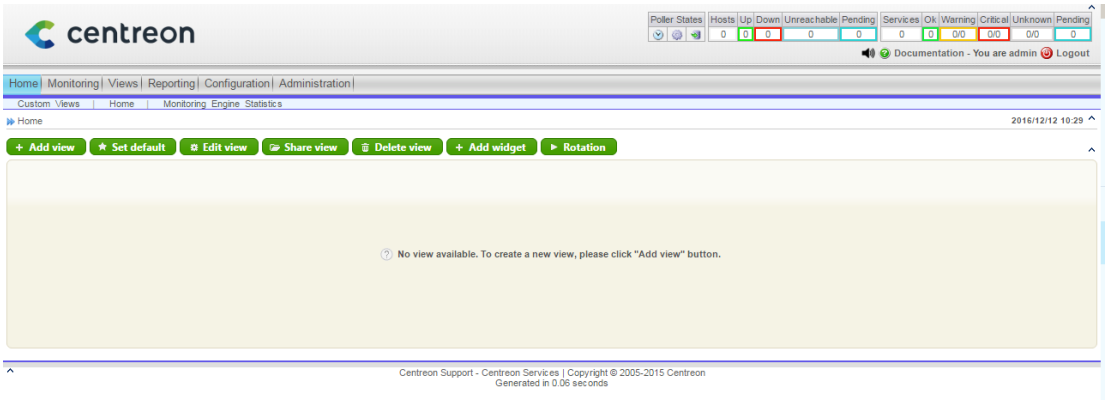

Figura 24 – Interface principal do Centreon após o primeiro login

Abaixo do logotipo do Centreon, se localiza o **menu principal**, mostrado na figura 25. Cada um dos itens deste menu possui subitens, cuja descrição se vê logo abaixo:

a) **Home**
   - **Custom views**: Mostra visualizações customizadas de hosts. É também a tela padrão do Centreon, que aparece logo após o login ser efetuado.
   - **Home**: Mostra uma visão geral dos status dos hosts e dos serviços, bem como dos problemas de hosts e de serviços que ainda não foram resolvidos.
   - **Monitoring Engine Statistics**: Mostra estatísticas sobre o processo de checagem efetuado pela ferramenta de monitoramento.

b) **Monitoring**
   - **Services**: Mostra a lista de serviços monitorados por host.
   - **Hosts**: Mostra a lista de hosts monitorados
   - **Event Logs**: Mostra os logs relativos a eventos do monitoramento, como avisos gerais, erros críticos e mudanças de status de hosts e serviços.

c) **Views**
   - **Graphs**: Permite ver gráficos de desempenho para os serviços monitorados de cada host.

d) **Reporting**
   - **Dashboard**: Permite ver dashboards com estatísticas de monitoramento relativas a hosts, grupos de hosts ou grupos de serviços.

e) **Configuration**
   - **Hosts**: Permite adicionar e remover hosts, bem como alterar suas configurações.
   - **Services**: Permite adicionar e remover serviços, bem como alterar suas configurações.
   - **Users**: Permite adicionar e remover usuários, bem como alterar suas configurações.
   - **Commands**: Permite adicionar e remover comandos de checagem, bem como

alterar suas configurações.

- **Notifications**: Permite adicionar e remover notificações, bem como alterar suas configurações.
- **SNMP Traps**: Permite adicionar e remover traps, bem como alterar suas configurações.
- **Monitoring Engines**: Permite validar mudanças nas configurações e reiniciar o sistema caso não haja erros.
- **Centreon**: Permite verificar informações sobre o status do servidor do Centreon (não relativas ao monitoramento principal).

f) **Administration**

- **Options**: Permite configurar as opções gerais do Centreon.
- **Extensions**: Permite verificar o status das extensões (módulos que adicionam funcionalidades extras ao Centreon).
- **ACL**: Permite configurar listas de controle de acesso (Access Control Lists), que limitam o acesso de usuários à interface do Centreon através de um conjunto de regras.
- **Logs**: Permite ver o histórico de mudanças aplicadas ao sistema, como adições, modificações e deleções de hosts, serviços e usuários.
- **Sessions**: Permite ver quais são os usuários atualmente conectados ao Centreon.
- **Server Status**: Permite ver dados relativos ao sistema operacional, à configuração de hardware, ao uso de memória e ao uso de disco do servidor em que o Centreon está instalado.
- **About**: Permite ver os créditos dos desenvolvedores da versão do Centreon utilizada.

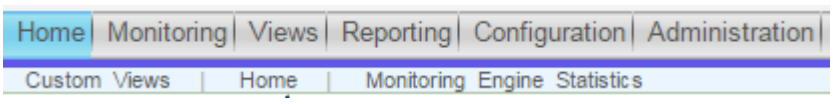

Figura 25 – Menu principal do Centreon.

A barra superior, mostrada na figura 26, se localiza no canto superior direito da

interface principal e permite visualizar rapidamente o número de hosts e serviços configurados, bem como quais destes possuem cada tipo de status.

Os tipos de status que cada host ou serviço pode assumir são descritos abaixo:

- **Up**: O host está funcionando normalmente.
- **Down**: O host está fora de funcionamento.
- **Unreachable**: O host está inalcançável.
- **Ok**: O serviço está funcionando normalmente.
- **Warning**: O serviço chegou ao nível de aviso.
- **Critical**: O serviço chegou ao nível crítico.
- **Unknown**: O status do serviço é desconhecido.
- **Pending**: O status do host ou do serviço ainda não foi checado.

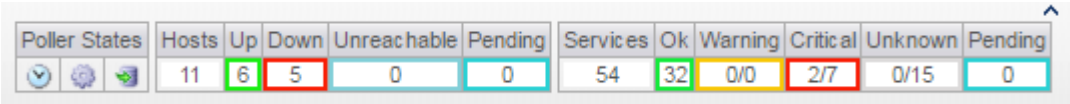

Figura 26 – Barra superior do Centreon.

4.2.2. Configuração de hosts e serviços

Para que o Centreon possa efetuar o monitoramento de hosts e serviços, é preciso configurá-los no sistema. O processo de configuração de hosts e serviços no Centreon é facilitado através do sistema de templates (modelos), que são um conjunto de configurações que podem ser aplicadas a todos os hosts que utilizam um template de host e a todos os serviços que utilizam um template de serviço.

4.2.2.1. Criação e visualização de hosts

Segundo Ribeiro (2015), para se criar um template de host, deve-se clicar em *Configuration* no menu principal e, depois, clicar em *Hosts* no submenu. No menu da esquerda, deve-se clicar em *Templates*. Aparecerá a tela da qual é mostrada uma parte na figura 27.

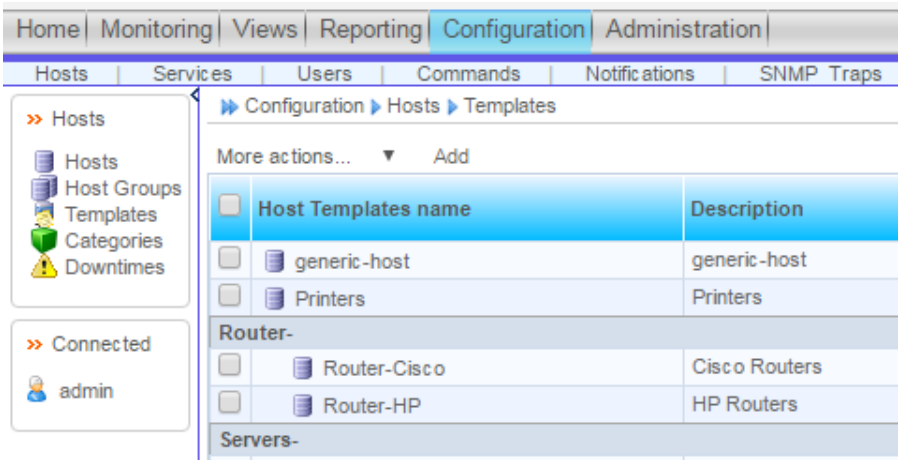

Figura 27 – Lista de templates de host do Centreon.

O item *Add* permite adicionar um novo template de host. Ao se clicar nele, aparecerá a tela mostrada na figura 28.

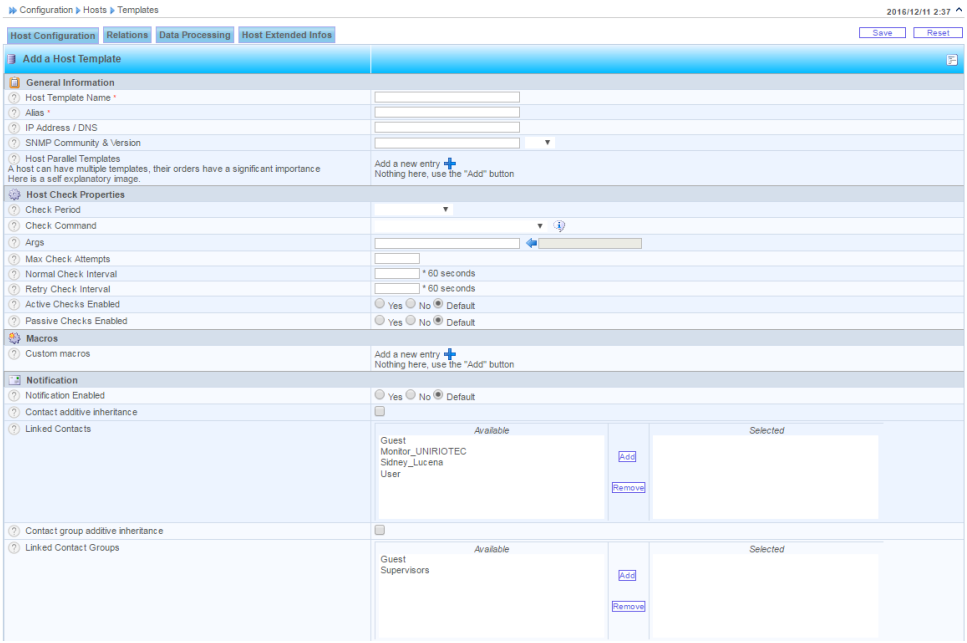

Figura 28 – Tela de criação de templates de host do Centreon.

Para a configuração de hosts da rede da Escola de Informática Aplicada que utilizem o sistema operacional Linux, foi criado um template com os seguintes dados:

- **Host Template Name:** Uniriotec-Linux
- **Alias:** Máquinas Uniriotec Linux
- **SNMP Community & Version:** UNIRIOTEC / 2c
- **Check Period:** 24x7

- **Check Command:** check_host_alive
- **Max Check Attempts:** 3
- **Normal Check Interval (* 60 seconds):** 1
- **Retry Check Interval (* 60 seconds):** 1
- **Notification Enabled:** Yes
- **Linked Contacts:** Monitor_UNIRIOTEC (administrador)
- **Linked Contact Groups:** Supervisors

Para criar um host, deve-se acessar o item *Hosts* do submenu do item *Configuration* do menu principal; o submenu já estará habilitado, não se precisando clicar em *Configuration*. Aparecerá a tela mostrada na figura 29.

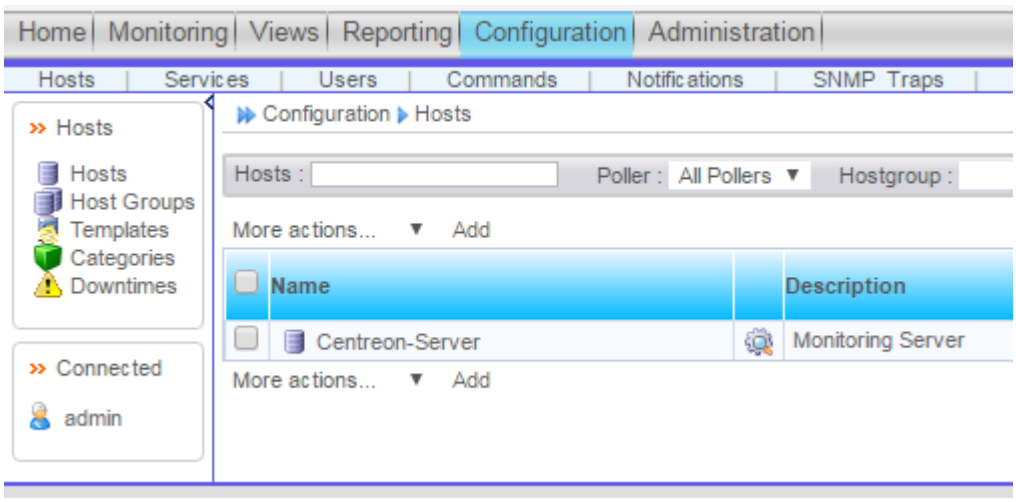

Figura 29 – Tela de criação de templates de host do Centreon.

O item *Add* permite adicionar um novo host. Ao se clicar nele, aparecerá uma tela igual à tela de adição de templates de hosts; uma parte dela está representada na figura 30. Como os hosts a serem criados seguirão o template *Uniriotec-Linux* e a maioria das configurações já foi feita no ato de criação do template, basta inserir o nome do host, seu alias e seu endereço IP ou DNS e indicar o template na opção *Host Templates* clicando em *Add a new entry* e escolhendo o nome do template desejado (no caso, *Uniriotec-Linux)*. Todas as outras configurações que foram especificadas no template serão automaticamente aplicadas ao host criado.

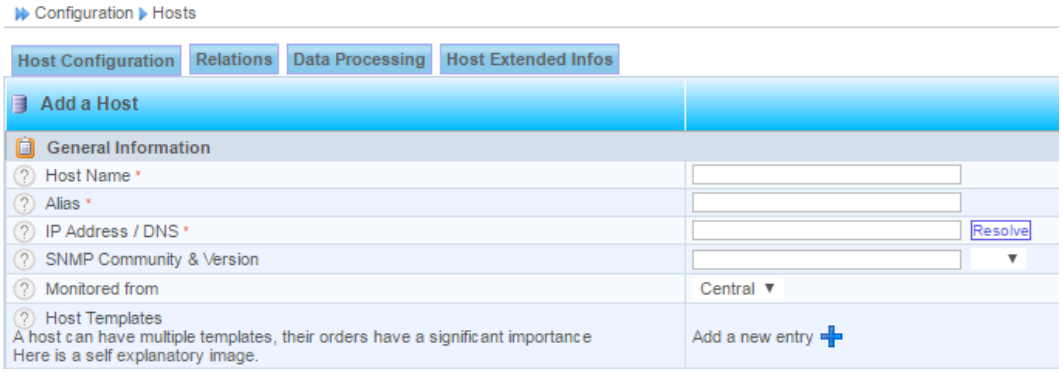

Figura 30 – Tela de criação de hosts do Centreon.

Para este trabalho, foram configurados os seguintes servidores Linux pertencentes à rede da EIA:

a) Servidor do Moodle

Nome: moodle-producao-02

Nome no Centreon: SERVER-moodle-producao-02

Endereço IP: 10.0.21.28

b) Servidor de testes do Moodle

Nome: teste-novo-servidor-moodle-2016

Nome no Centreon: SERVER-teste-novo-servidor-moodle-2016

Endereço IP: 10.0.1.28

c) Servidor do SAT (sistema de abertura de chamados)

Nome: servidor-sat-uniriotec

Nome no Centreon: SERVER-servidor-sat-uniriotec

Endereço IP: 10.0.21.30

d) Servidor de hospedagem da página web do portal do BSI

Nome: novo-portal-bsi

Nome no Centreon: SERVER-novo-portal-bsi

Endereço IP: 10.0.0.29

e) Servidor de backups

Nome: servidor-backup

Nome no Centreon: SERVER-servidor-backup

Endereço IP: 10.0.0.29

Para verificar o status dos hosts configurados após as inclusões destes terem sido efetuadas, deve-se acessar a tela geral de hosts (mostrada na figura 31) clicando-se no item *Hosts* do submenu do item *Configuration* e, depois, clicando-se em *Hosts* no menu à esquerda.

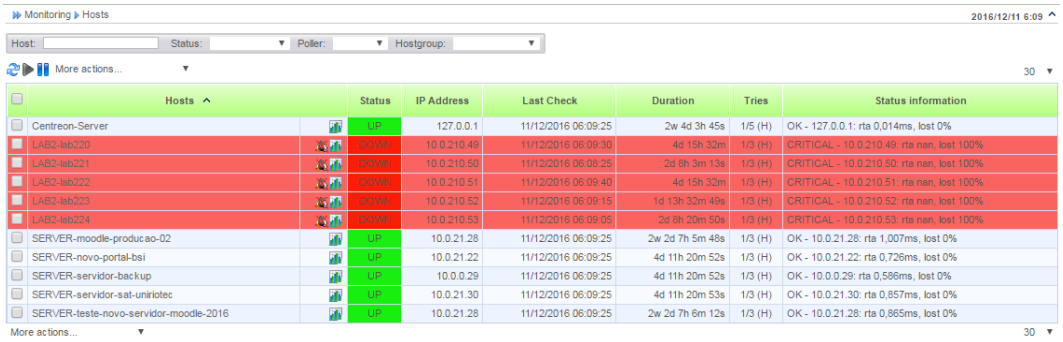

Figura 31 – Tela de visualização de hosts do Centreon.

4.2.2.2. Criação e visualização de serviços

Segundo Ribeiro (2015), para se criar um template de serviço, deve-se clicar em *Configuration* no menu principal e, depois, clicar em *Services* no submenu. No menu da esquerda, deve-se clicar em Templates. Aparecerá a tela da qual é mostrada uma parte na figura 32.

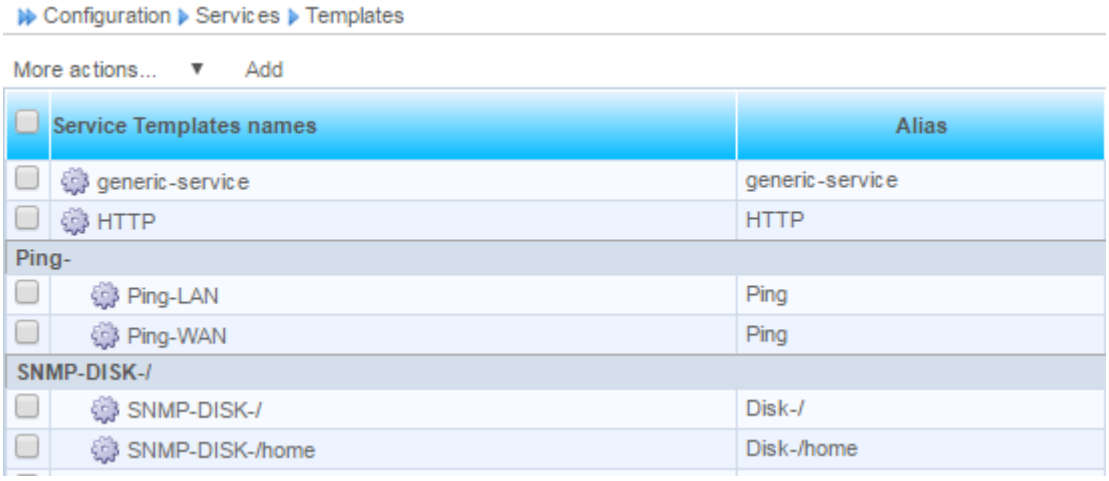

Figura 32 – Lista de templates de serviço do Centreon.

O item *Add* permite adicionar um novo template de serviço. Ao se clicar nele, aparecerá a tela da qual uma parte é mostrada na figura 33.

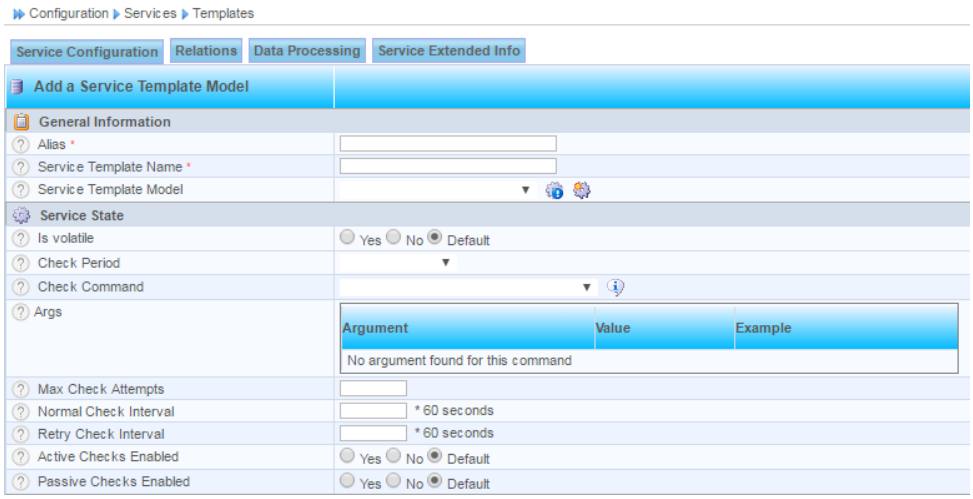

Figura 33 – Tela de inclusão de templates de serviço do Centreon.

Para este trabalho, foi configurado um serviço relativo ao monitoramento de tráfego na interface de rede principal de cada servidor. Como quatro dos cinco servidores utilizam a interface de rede *eth0*, foi criado um template de serviço baseado nela; para o servidor restante, que utiliza a interface de rede *ens32*, foi preciso realizar o processo alternativo de configurar o serviço sem utilizar um template, que será explicado mais à frente.

O template do serviço foi configurado da seguinte forma:

- **Alias:** Linux-Traffic-eth0
- **Service Template Name:** SNMP-Linux-Traffic-eth0
- **Check Command:** check_centreon_traffic
    - **interface:** eth0
    - **warning:** 80
    - **critical:** 90

Como um template também pode herdar configurações de outro template, as outras configurações do template SNMP-Linux-Traffic-eth0 foram feitas através do template *generic-service*:

- **Max Check Attempts:** 3
- **Normal Check Interval (* 60 seconds):** 5
- **Retry Check Interval (* 60 seconds):** 1
- **Active Checks Enabled:** Default
- **Passive Checks Enabled:** Default
- **Notification Enabled:** Yes
- **Linked Contacts:** Monitor_UNIRIOTEC (administrador)
- **Linked Contact Groups:** Supervisors

Para aplicar o template a vários hosts de uma só vez, é preciso clicar na aba *Relations* e, então, associar os hosts desejados ao template, como mostrado na figura 34.

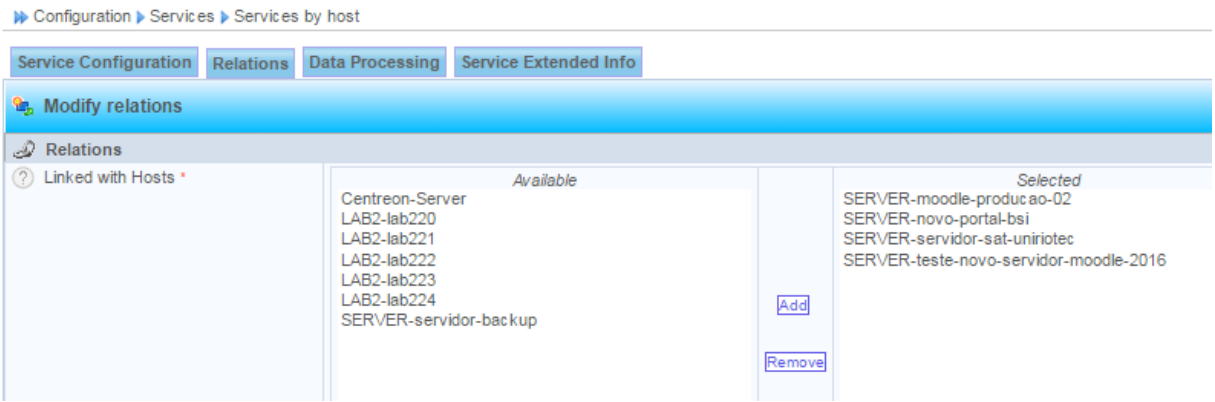

Figura 34 – Associação de hosts a um template de serviço no Centreon.

É preciso também configurar o tipo de gráfico, que será útil na análise do monitoramento. Para isso, deve-se clicar na aba *Service Extended Info* e mudar a opção *Graph*

Template para *Traffic*, como visto na figura 35.

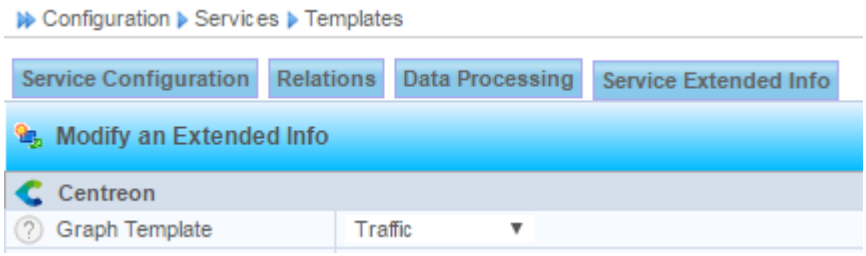

Figura 35 – Associação de um template de gráfico a um template de serviço no Centreon.

Como citado anteriormente, um dos servidores usa uma interface de rede diferente da interface *eth0* e, por isso, não pode utilizar o template criado para ela. Este servidor é o servidor de backup (denominado *SERVER-servidor-backup* no Centreon) e, para ele, o processo efetuado foi o que é descrito abaixo, segundo Ribeiro (2015):

a) Acessar a lista de serviços por host (clicar em *Configuration* no menu principal, depois em *Services* no submenu e depois em *Services by host* no menu da esquerda).

b) Clicar na caixa de seleção em qualquer uma das linhas que contenham o serviço de nome *Traffic-Linux-eth0*.

c) Na caixa de opções *More actions…*, localizada tanto acima quanto abaixo da lista de hosts, escolher a opção *Duplicate*. Na caixa de diálogo que surgirá perguntando *Do you confirm the duplication?*, clicar em *OK*.

d) Na lista de hosts, clicar no nome do serviço duplicado. Surgirá a tela de modificação do serviço.

e) Modificar o nome do serviço para *Traffic-Linux-ens32* e o argumento *interface* do comando de checagem *check_centreon_traffic* para *ens-32*.

f) Clicar na aba *Relations* e deixar somente o servidor *SERVER-servidor-backup* na lista *Selected*.

g) Clicar na aba *Service Extended Info* e modificar o tipo de gráfico para *Traffic*.

h) Clicar no botão *Save*, localizado à extrema direita das abas.

Para visualizar a lista de hosts com todos os novos serviços criados, basta seguir o procedimento citado no item anterior.

4.2.2.3. Salvamento de configurações

Para se salvar e aplicar as configurações de hosts, templates de hosts, serviços e templates de serviços criadas, deve-se seguir o procedimento abaixo, segundo Ribeiro (2015):

- Clicar em *Configuration* no menu principal e depois em *Monitoring Engines* no submenu.

- Na tela mostrada na figura 36 as ações *Generate Configuration Files* e *Run monitoring engine debug (-v)* já estarão marcadas por padrão. Clicar no botão *Export*.

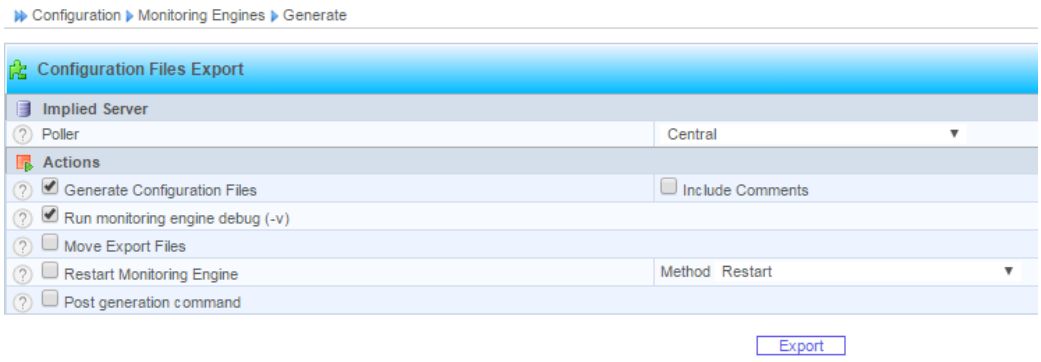

Figura 36 – Tela de salvamento de configurações do Centreon.

A seção *Console* aparecerá na parte de baixo da tela indicando se houve erros nas configurações. Caso não haja nenhum erro, desmarcar as duas opções da lista *Actions* já marcadas e marcar as três restantes (*Move Export Files*, *Restart Monitoring Engine* e *Post generation command*). Clicar novamente no botão *Export*.

- A seção *Console* aparecerá novamente. Caso não haja erros, basta verificar o funcionamento das novas configurações.

Esse procedimento deve ser feito também após qualquer outro tipo de modificação nas configurações.

4.2.3. Configuração de alertas

Como mencionado anteriormente, uma das premissas de um sistema de monitoramento é tornar possível que o setor responsável pela infraestrutura da organização no qual o sistema está implantado esteja ciente dos problemas que possam ocorrer na rede da organização – seja um problema de indisponibilidade de servidores, de indisponibilidade de conexão de Internet ou de um computador pertencente à rede (espaço em disco prestes a terminar, uso de memória RAM em excesso, dentre outros), seja esse computador um servidor ou não. Esse processo é facilitado pelo uso de alertas, que são mensagens enviadas por e-mail contendo informações sobre os problemas.

4.2.3.1. Configuração de contatos

Primeiramente, é preciso cadastrar no sistema todas as pessoas que irão receber os alertas. Segundo Ribeiro (2015), isso é feito da seguinte forma:

a) No menu superior do Centreon, clicar em *Configuration*. No submenu (barra abaixo do menu superior), clicar em *Users*. Aparecerá a tela de listagem de usuários, mostrada na figura 37, na qual se deve clicar em *Add*.

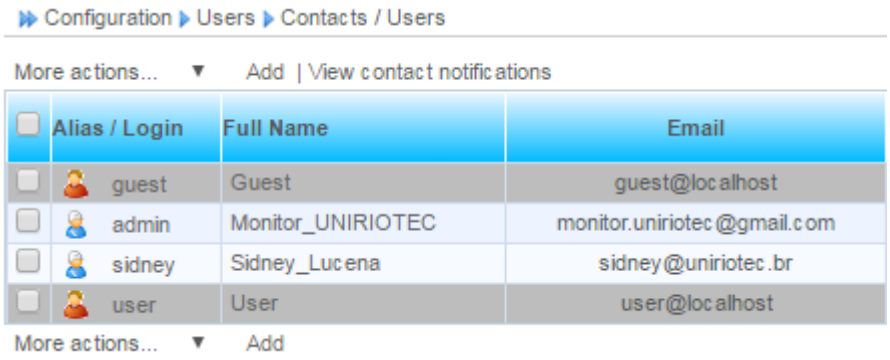

Figura 37 – Tela de listagem de usuários do Centreon

b) Surgirá a tela de inclusão de usuários, mostrada na figura 38.

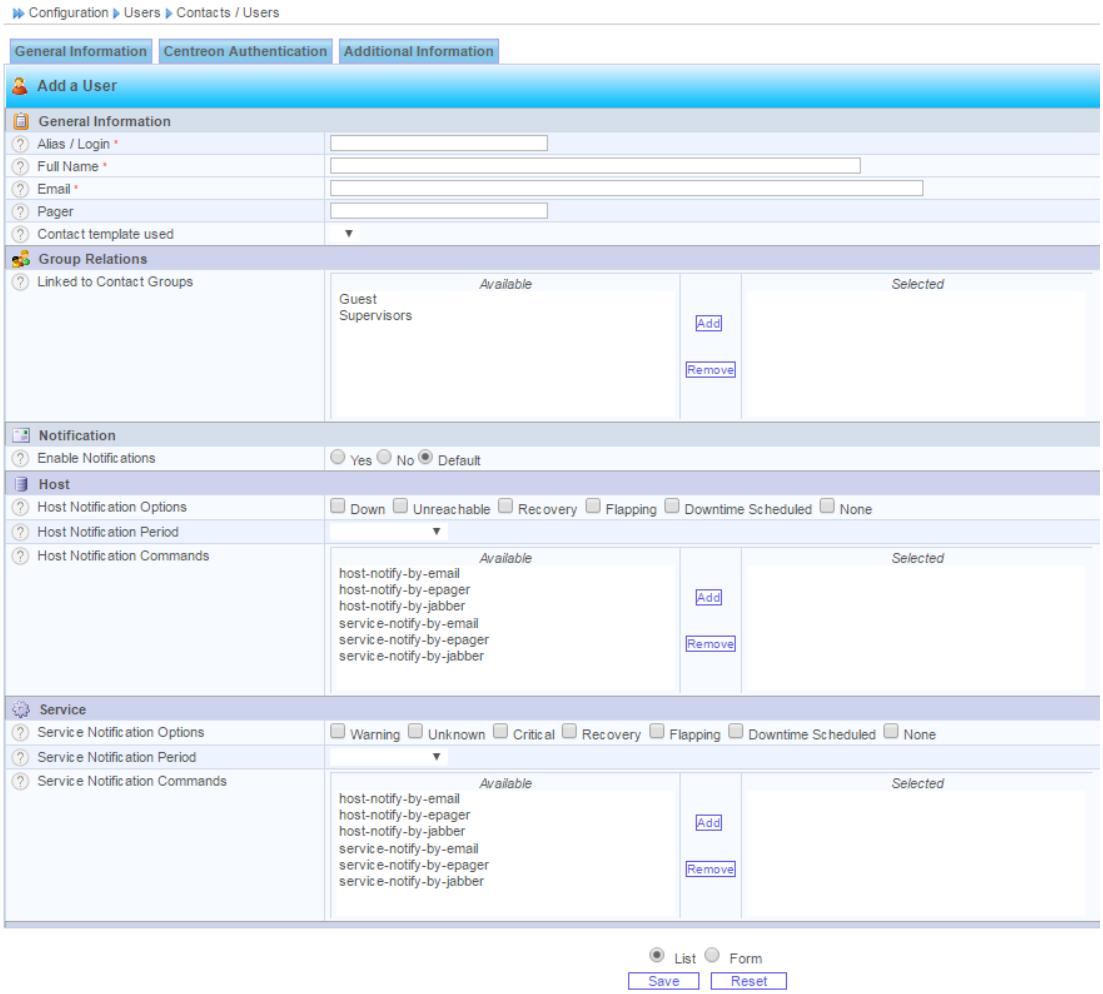

Figura 38 – Tela de inclusão de usuários do Centreon.

Nessa tela, deverão ser preenchidos os seguintes campos:

- *Alias / Login*: Nome de usuário a ser utilizado para login no sistema.
- *Full Name*: Nome completo do contato.
- *Email*: Endereço de e-mail utilizado pelo contato.
- *Host Notification Period*: A opção *24x7* permite que o contato receba alertas relativos a hosts 24 horas por dia e 7 dias por semana, sempre que estes forem emitidos.
- *Host Notification Commands*: Comandos que serão usados para enviar alertas relativos a hosts ao contato. A coluna *Available* mostra todos os comandos disponíveis e a coluna *Selected* mostra os comandos escolhidos para esta opção; para mover um comando da primeira para a segunda, deve-se clicar em seu nome e, depois, no botão *Add*. Para que o contato receba alertas via e-mail, deve-se selecionar o comando *host-notify-by-email*.
- *Service Notification Period*: Idem ao item *Host Notification Period*, mas em relação a serviços.
- *Service Notification Command*: Idem ao item *Host Notification Command*, mas em relação a serviços.

Após efetuar as mudanças, clique no botão *Save* e siga o procedimento de confirmação de mudanças de configurações descrito no item 4.2.2.3.

4.2.3.2. Configuração de grupos de contatos

Caso necessário, os contatos podem ser organizados em grupos para facilitar a configuração de alertas. Pode ser criado, por exemplo, um grupo para a diretoria da organização e outra para o setor de infraestrutura, de modo que não seja preciso selecionar os contatos um a um na hora de configurar as notificações para os serviços de um novo host.

Segundo Ribeiro (2015), o processo para configuração de grupos de contatos é o descrito a seguir:

a) No menu superior do Centreon, clicar em *Configuration*. No submenu (barra abaixo do menu superior), clicar em *Users*. No menu da esquerda, clicar em *Contact Groups*. Aparecerá a tela de listagem de grupos de contatos, mostrada na figura 39, na qual se deve clicar em *Add*.

Figura 39 – Tela de listagem de grupos de contatos do Centreon.

b) Surgirá a tela de inclusão de grupos de contatos, mostrada na figura 40.

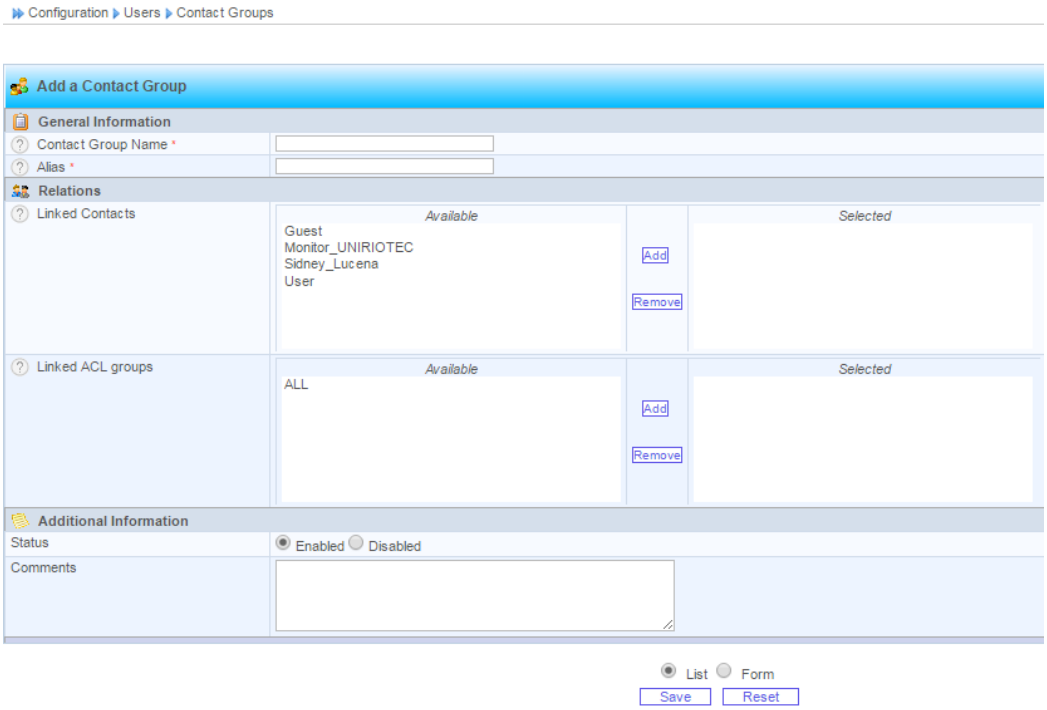

Figura 40 – Tela de inclusão de grupos de contatos do Centreon.

Nessa tela, deve-se preencher os seguintes campos:

- *Contact Group Name*: Nome do grupo de contatos
- *Alias*: Descrição do grupo de contatos

- *Linked Contacts*: Contatos a serem incluídos no grupo. A coluna *Available* mostra todos os contatos (usuários) disponíveis e a coluna *Selected* mostra os contatos escolhidos para esta opção; para mover um contato da primeira para a segunda, deve-se clicar em seu nome e, depois, no botão *Add*.

Após efetuar as mudanças, clique no botão *Save* e siga o procedimento de confirmação de mudanças de configurações descrito no item 4.2.2.3.

4.2.3.3. Configuração de serviços para emitirem alertas

No Centreon, os alertas podem ser configurados por serviço; ou seja, cada serviço dentro de um host pode ter seu próprio perfil de alerta (usuários notificados, período de notificação, dentre outros parâmetros). É possível também configurar alertas para templates de serviço, de forma que todos os serviços configurados utilizando os templates em questão passem a utilizar o perfil de alerta configurado dentro destes.

Uma vez que neste trabalho foram utilizados templates de serviço para os serviços de cada host, será explicado o processo de configuração de alertas em templates de serviço, que, segundo Ribeiro (2015), acontece da seguinte forma, com as mesmas telas mostradas no passo-a-passo para configuração de templates de serviços (seção 3.6.2):

a) No menu superior do Centreon, clicar em *Configuration*. No submenu (barra abaixo do menu superior), clicar em *Services*. No menu da esquerda, clicar em *Templates*. Surgirá a tela de listagem de templates de serviço.

b) Localizar o template de serviço para o qual se deseja configurar os alertas e clicar em seu nome. Surgirá a tela de configuração do template, mostrada na figura X.

c) Na tela de configuração do serviço, preencher os seguintes campos:

- *Check Period*: A opção *24x7* permite que a verificação dos serviços – bem como o consequente envio de alertas caso o serviço esteja dentro dos níveis de alerta especificados - possa acontecer 24 horas por dia e 7 dias por semana.

Esta é a rotina mais recomendada, pois os servidores de uma organização não costumam ser desligados fora de dias úteis.

- *Args*: Este parâmetro permite que sejam especificados os argumentos utilizados pelo comando de checagem vinculado ao serviço. O template de serviço *SNMP-Disk-/* (utilizado pelo serviço *Disk-/*), por exemplo, possui vinculado o comando de checagem dois de seus argumentos os valores de alerta *Warning* (estado de alerta, no qual se deve começar a ter atenção ao serviço) e *Critical* (estado crítico, no qual se deve dar total atenção ao serviço). Nem todos os serviços possuem esses argumentos, mas os que possuem podem ser configurados.
- *Max Check Attempts*: Número máximo de tentativas de checagem antes de o status do serviço ser confirmado.
- *Normal Check Interval*: Intervalo (em minutos) entre checagens quando o serviço estiver com o status OK.
- *Retry Check Interval*: Intervalo (em minutos) entre checagens quando o serviço estiver com qualquer status que não seja OK.
- *Implied Contacts*: Contatos (usuários) que receberão as notificações de alertas referentes ao serviço. A coluna *Available* mostra todos os usuários disponíveis e a coluna *Selected* mostra os usuários escolhidos para esta opção; para mover um usuário da primeira para a segunda, deve-se clicar em seu nome e, depois, no botão *Add*.
- *Implied Contact Groups*: Grupos de contatos (usuários) que receberão as notificações de alertas referentes ao serviço. A coluna *Available* mostra todos os usuários disponíveis e a coluna *Selected* mostra os usuários escolhidos para esta opção; para mover um usuário da primeira para a segunda, deve-se clicar em seu nome e, depois, no botão *Add*.
- *Notification Interval*: Intervalo (em minutos) entre envios de e-mails de notificações de alertas para o serviço.
- *Notification Period*: Período em que os e-mails de notificações de alertas para o serviço podem ser enviados. Assim como em relação ao parâmetro *Check Period*, é recomendável a configuração *24x7*.

Após efetuar as mudanças, clique no botão *Save* e siga o procedimento de confirmação de mudanças de configurações descrito no item 4.2.2.3.

4.2.3.4. Exemplos de alertas recebidos

Neste item serão mostrados alguns exemplos de e-mails de alerta que podem ser recebidos.

A figura 41 mostra um alerta de serviço com status *UNKNOWN*.

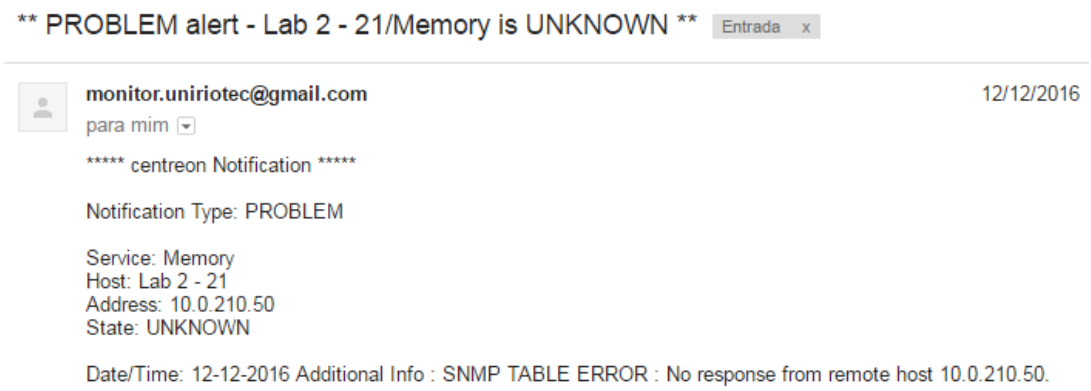

Figura 41 – Exemplo de alerta de serviço do Centreon com status *UNKNOWN*.

A figura 42 mostra um alerta de serviço com status OK.

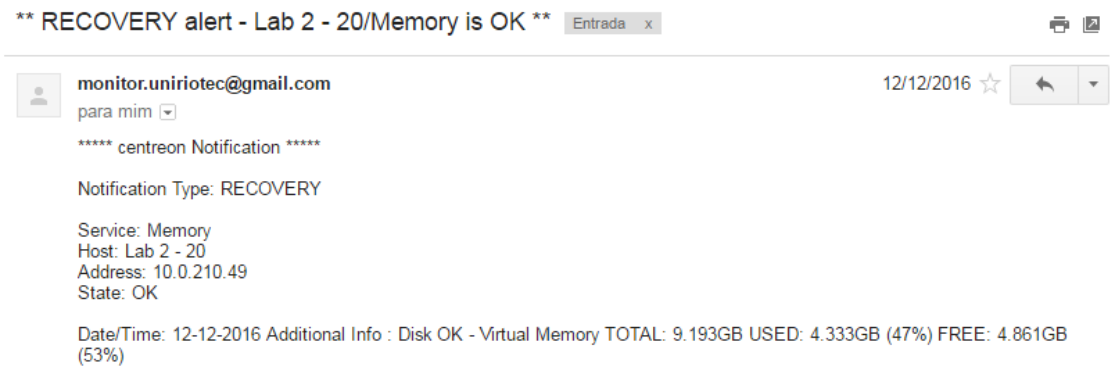

Figura 42 – Exemplo de alerta de serviço do Centreon com status *OK*.

A figura 43 mostra um alerta de serviço com status CRITICAL.

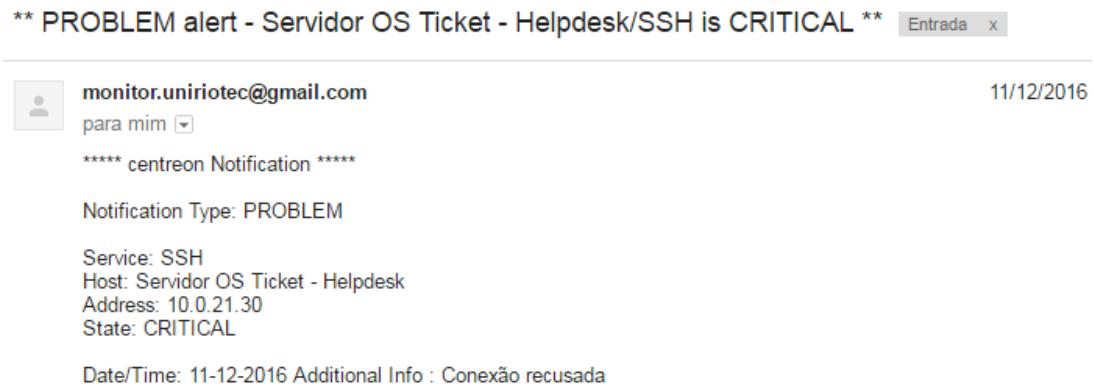

Figura 43 – Exemplo de alerta de serviço do Centreon com status *CRITICAL*.

A figura 44 mostra um alerta de host com status *DOWN* (host indisponível).

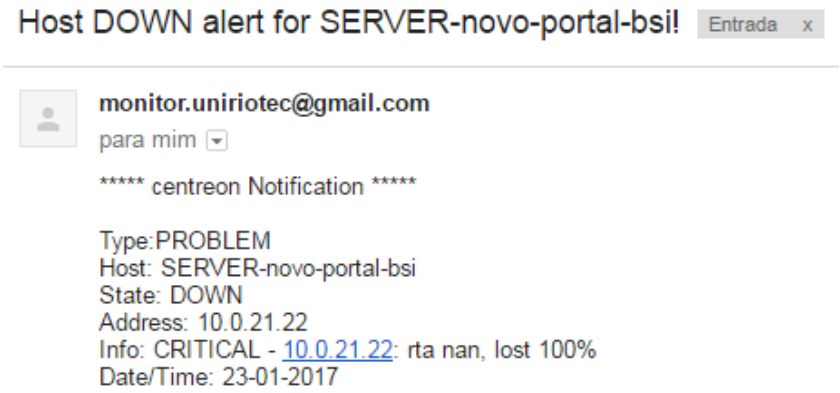

Figura 44 – Exemplo de alerta de host do Centreon com status *DOWN*.

A figura 45 mostra um alerta de host do tipo *Up* (host disponível), que é enviado após o host estar disponível novamente.

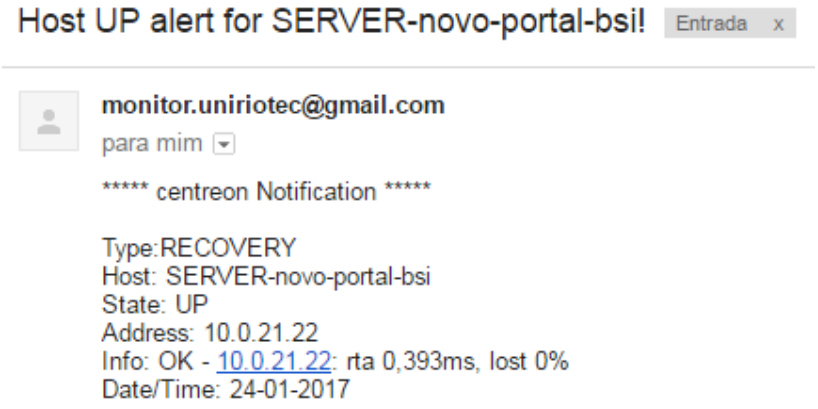

Figura 45 – Exemplo de alerta de host do Centreon com status *UP*.

4.2.4. Configuração de gráficos

Caso o usuário deseje, é possível customizar os gráficos exibidos pelo Centreon. Isso pode ser feito de duas formas: Configurando templates de gráficos e configurando curvas[14] de gráficos.

4.2.4.1. Configuração de templates de gráficos

a) No menu superior do Centreon, clicar em *Views* e, depois, em *Graphs*. No menu da esquerda, clicar em *Templates*. Aparecerá a listagem de templates de gráficos, mostrada na figura 46.

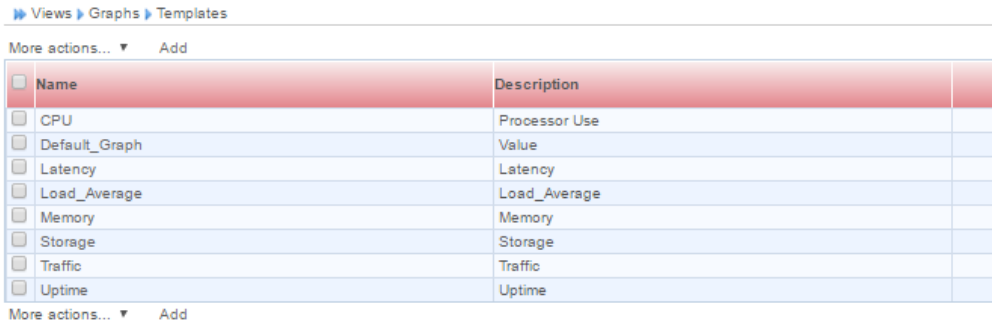

Figura 46 – Tela de listagem de templates de gráficos do Centreon.

b) Ao se clicar no nome de um template de gráfico, podem ser vistas as opções de customização referentes a ele, numa listagem ilustrada pela figura 47.

[14] Linha que representa a variação dos dados dentro de certo período de tempo.

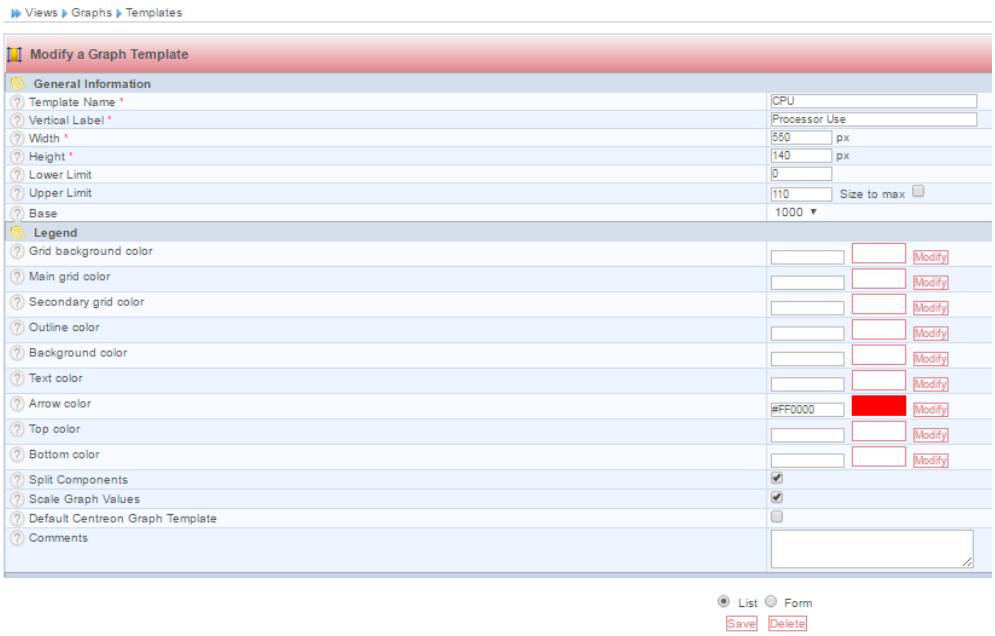

Figura 47 – Tela de configuração de templates de gráficos do Centreon.

Abaixo segue a descrição das opções configuráveis:

- *Template Name*: Nome do template.
- *Vertical Label*: Legenda do eixo Y do gráfico.
- *Width*: Largura do gráfico (em pixels).
- *Height*: Altura do gráfico (em pixels).
- *Lower limit*: Limite inferior (mínimo) do eixo Y do gráfico.
- *Upper limit*: Limite superior (máximo) do eixo Y do gráfico.
- *Base*: Base de cálculo para o escalonamento do eixo Y do gráfico. A opção *1000* é utilizada para medidas na proporção 1:1000 (1 kV = 1000 volts, por exemplo), enquanto a opção *1024* é usada para medidas na proporção 1:1024 (1 KB = 1024 bytes, por exemplo).
- *Grid background color*: Cor de fundo da grade.
- *Main grid color*: Cor da grade principal.
- *Secondary grid color*: Cor da grade secundária.
- *Outline color*: Cor do contorno.
- *Background color*: Cor de fundo.
- *Text color*: Cor do texto.
- *Arrow color*: Cor das setas dos eixos X e Y.

- *Top color*: Cor da borda superior e da borda esquerda do gráfico
- *Bottom color*: Cor da borda inferior e da borda esquerda do gráfico
- *Split Components*: Se essa opção estiver marcada, as curvas serão automaticamente separadas.
- *Scale Graph Values*: Se essa opção estiver marcada, o gráfico será automaticamente escalonado.
- *Default Centreon Graph Template*: Se essa opção for marcada, o template se torna o template padrão do Centreon – ou seja, será o template aplicado a qualquer gráfico para o qual não foi definido um modelo.
- *Comments*: Permite inserir comentários.

4.2.4.2. Configuração de curvas de gráficos

a) No menu superior do Centreon, clicar em *Views* e, depois, em *Graphs*. No menu da esquerda, clicar em *Curves*. Aparecerá a listagem de curvas de gráficos, mostrada na figura 48.

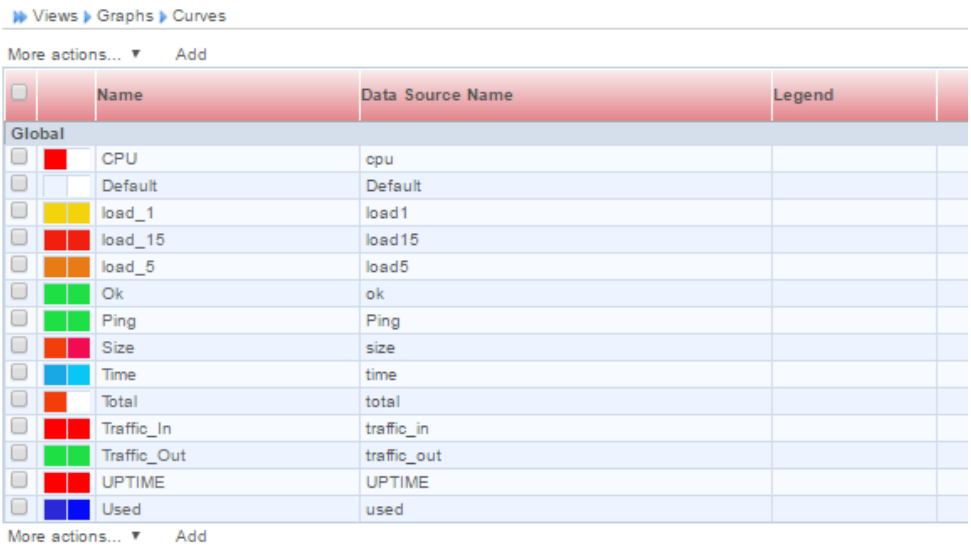

Figura 48 – Tela de listagem de curvas de gráficos do Centreon.

b) Ao se clicar no nome de uma curva, podem ser vistas as opções de customização referentes a ela, numa listagem ilustrada pela figura 49.

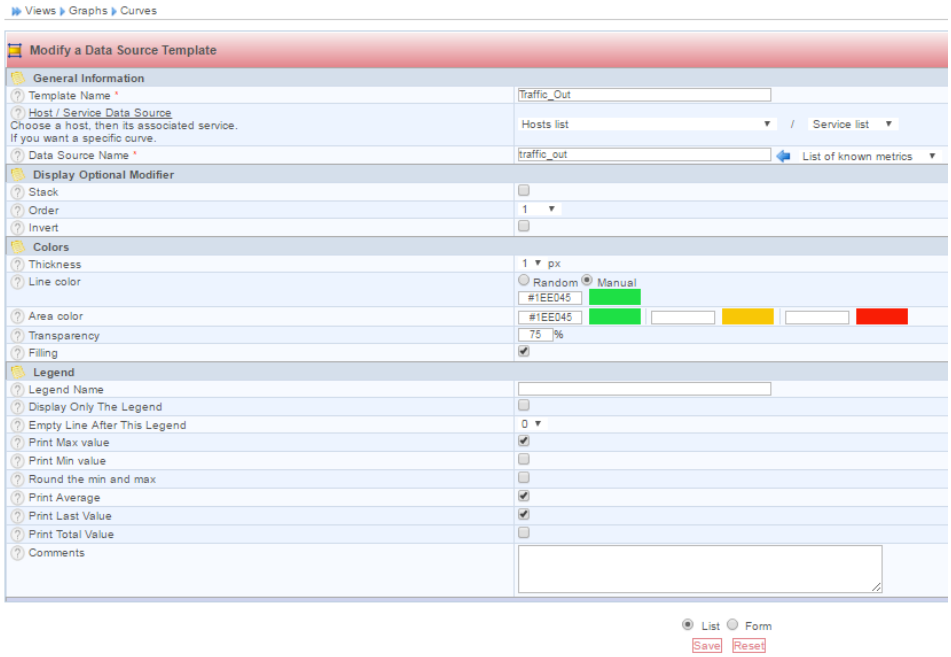

Figura 49 – Tela de configuração de curvas de gráficos do Centreon.

Abaixo segue a descrição das opções configuráveis:

- *Template Name*: Nome do template.
- *Host / Service Data Source*: Host ou serviço para o qual a curva será usada. Se essa opção não for preenchida, a curva será aplicada a todos os serviços em que a métrica aparece.
- *Data Source Name*: Métrica que usará a curva.
- *Stack*: Se essa opção for marcada, a curva será empilhada em relação às outras. Útil para verificar a proporção de uma métrica em relação a outra.
- *Order*: Define a ordem de empilhamento da curva em relação às outras. Quanto menor o número, mais perto do eixo X ela estará.
- *Invert*: Se essa opção for marcada, a curva será invertida em relação ao eixo Y, apresentando um valor oposto em relação ao valor absoluto. Útil para, por exemplo, verificar a proporção do tráfego de entrada em relação ao tráfego de saída.
- *Thickness*: Grossura da curva (em pixels).
- *Line color*: Cor da curva.
- *Area color*: Cor do preenchimento da curva, em caso de a opção *Filling*, descrita mais abaixo, estar marcada. Contém três valores,

correspondentes às cores dos status *OK*, *WARNING* e *CRITICAL*, respectivamente.

- *Transparency*: Nível de transparência da cor do contorno da curva.
- *Filling*: Se essa opção for marcada, a curva será totalmente preenchida com a cor de de preenchimento definida de acordo com o status.
- *Legend Name*: Legenda da curva.
- *Display Only The Legend*: Se essa opção for marcada, a curva não aparecerá e somente a legenda será visível.
- *Empty Line After This Legend*: Número de linhas vazias (entre 0 e 3) que aparecerá após a legenda.
- *Print Max value*: Se essa opção for marcada, será mostrado na legenda o valor do ponto de máximo alcançado pela curva.
- *Print Min value*: Se essa opção for marcada, será mostrado na legenda o valor do ponto de mínimo alcançado pela curva.
- *Round the min and max*: Se essa opção for marcada, os valores dos pontos de mínimo e de máximo serão arredondados.
- *Print Average*: Se essa opção for marcada, será mostrada na legenda a média dos valores dos pontos da curva.
- *Print Last Value*: Se essa opção for marcada, será mostrado na legenda o valor do último ponto da curva.
- *Print Total Value*: Se essa opção for marcada, será mostrado o valor total da curva (soma de todos os valores dos pontos da curva no período selecionado).
- *Comments*: Permite inserir comentários na legenda.

Caso sejam efetuadas mudanças, clique no botão *Save* e siga o procedimento de confirmação de mudanças de configurações descrito no item 4.2.2.3.

A figura 50 apresenta um exemplo de gráfico com curvas empilhadas.

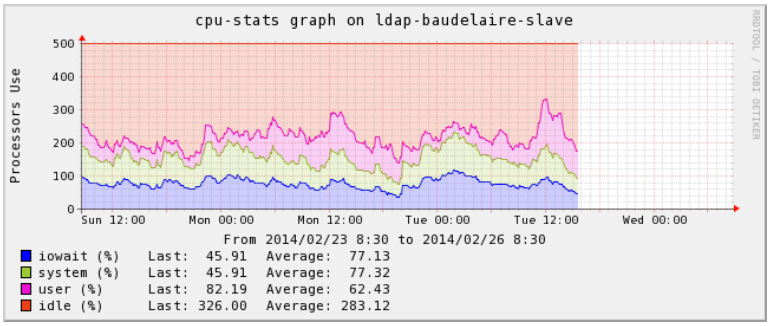

Figura 50 – Exemplo de gráfico do Centreon com curvas empilhadas.

A figura 51 apresenta um exemplo de gráfico com curvas invertidas.

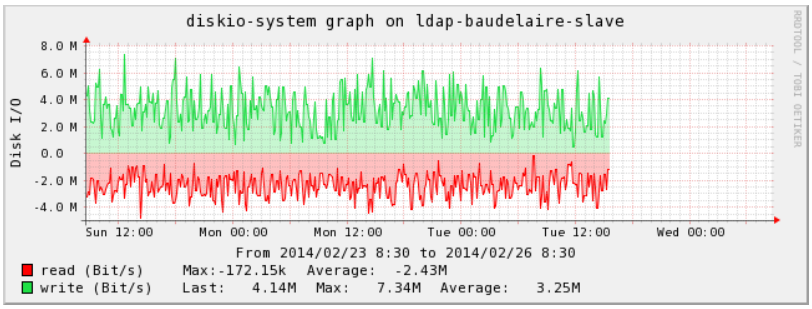

Figura 51 – Exemplo de gráfico do Centreon com curvas invertidas.

A figura 52 apresenta um exemplo de gráfico contendo curvas com e sem preenchimento.

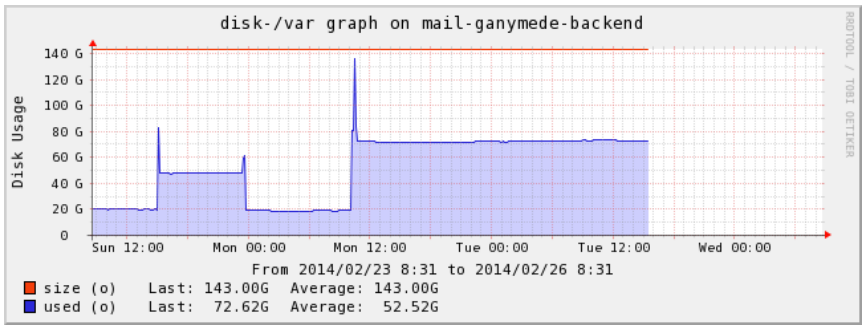

Figura 52 – Exemplo de gráfico do Centreon contendo curvas com e sem preenchimento.

5 Análise do tráfego de rede

Nenhum sistema de monitoramento de redes está completo sem a possibilidade de geração de gráficos de comportamento relativos aos serviços dos dispositivos gerenciados que estejam sendo monitorados, ainda que isso seja possível somente com a utilização de ferramentas de terceiros (como no Nagios, por exemplo). Com essa funcionalidade corretamente configurada, é possível analisar o histórico do comportamento de cada serviço, o que é essencial para que o setor responsável pela infraestrutura computacional de uma organização possa, caso necessário, promover correções e melhorias.

Segundo Vassallo (2012), o Centreon efetua o seguinte processo para salvar dados coletados e gerar gráficos com esses dados:

- O Centreon executa a checagem de um serviço.
- O Centreon executa o comando *process-service-perfdata*, que processa os dados coletados na checagem de serviço executada e cuja saída acontece em um arquivo denominado Service Performance Data File.
- O serviço Centstorage e a ferramenta RRDtool processam os dados do referido arquivo e os armazenam no banco de dados MySQL do Centreon e em arquivos RRD[15] localizados no servidor.
- O RRDtool é ativado quando o usuário utiliza a interface web para solicitar a visualização de gráficos, gerando os gráficos solicitados a partir dos dados armazenados.

No Centreon, os gráficos podem ser visualizados da seguinte forma:

a) No menu principal, clicar no item *Views* e, depois, clicar no item *Graphs* do submenu (o único existente). Surgirá a tela mostrada na figura 53.

[15] Segundo Yu (2012), o RRD (Round Robin Database) é um banco de dados de armazenamento que utiliza listas circulares para armazenar dados de séries temporais (dados que são observados em diferentes instantes de tempo) com maior precisão, sendo bastante utilizado para o armazenamento de dados estatísticos, cujas possibilidades de uso envolvem a geração de gráficos.

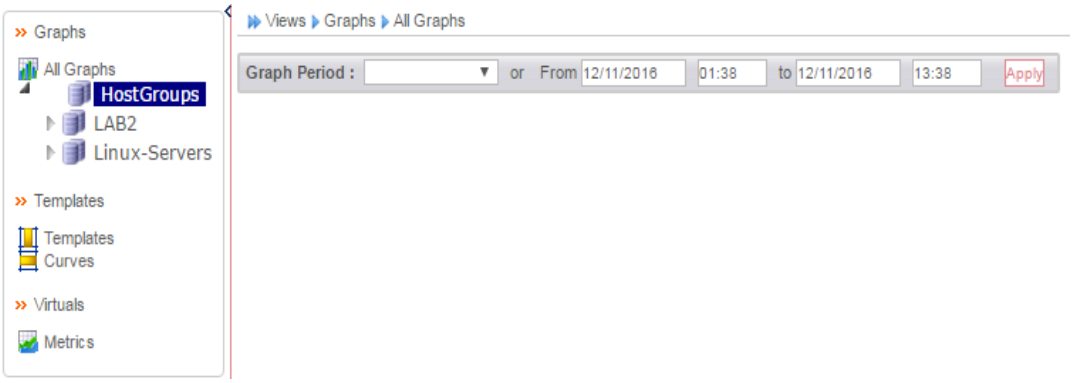

Figura 53 – Tela de visualização de gráficos do Centreon (vazia).

b) No menu da esquerda, clicar na seta ao lado do ícone do grupo *Linux-Servers*. Aparecerá uma lista contendo todos os hosts deste grupo (o servidor do Centreon e os cinco servidores adicionados). Clicando na seta ao lado do ícone de cada host, aparecerá a lista de serviços configurados para ele. É possível visualizar o gráfico de um serviço clicando na caixa de seleção ao lado deste, como mostrado na figura 54. Na barra acima da área do gráfico, é possível escolher o período de tempo em relação ao qual se deseja ver os dados.

Figura 54 – Tela de visualização de gráficos do Centreon.

Para a análise de monitoramento a ser feita neste capítulo, foi escolhido o serviço de tráfego, previamente configurado para cada um dos hosts determinados para fazer parte da análise. Este gráfico possui duas variáveis: A variável *traffic_in*, que registra o tráfego de entrada e é representada em vermelho, e a variável *traffic_out*, que registra o tráfego de saída e é representada em verde. Ambas as variáveis são medidas em bits por segundo (bps).

É importante ressaltar que a versão 2.6.4 do Centreon, utilizada neste trabalho, possui uma falha em relação ao gráfico de tráfego (template *Traffic*, configurado anteriormente para

os serviços *SNMP-Traffic-Linux-eth0* e *SNMP-Traffic-Linux-ens32*): Como a variável *traffic_in* possui valores negativos no gráfico, o ponto de máximo que a legenda do gráfico apresenta para essa variável é, na verdade, seu ponto de mínimo. Devido a isso, o ponto de máximo será apontado de forma aproximada.

5.1. Servidor do Moodle

Para a análise do servidor do Moodle, foi escolhido o período entre os dias 06/12 (primeiro dia em que o gráfico esteve disponível) e 10/12. O gráfico para esse período é mostrado na figura 55.

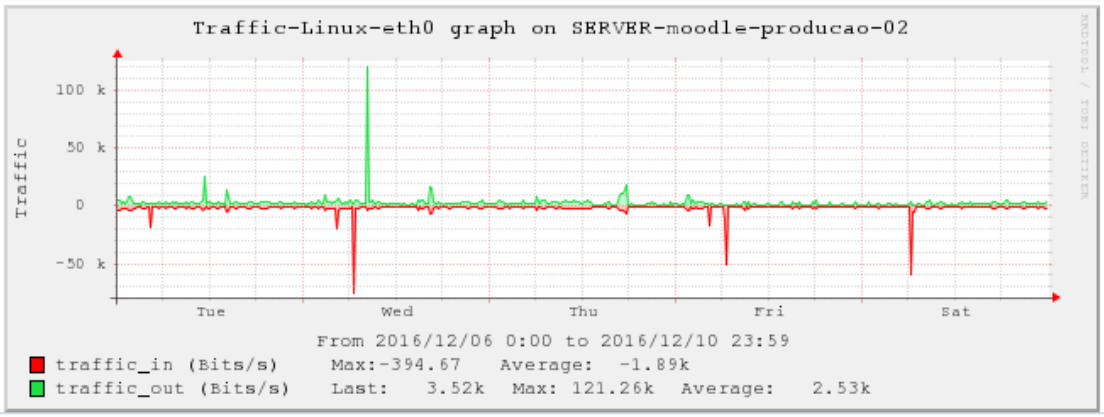

Figura 55 – Gráfico de tráfego do servidor do Moodle.

Como o Moodle é um sistema de disponibilização de conteúdo entre professores e alunos, é normal que tanto o tráfego de dados para dentro como o tráfego de dados para fora do servidor seja maior entre segundas-feiras e sextas-feiras. Foi verificado também um ponto de maior tráfego de entrada no dia 10/12; como este dia foi um sábado, existe a hipótese de um ou mais alunos ou professores terem enviado arquivos em grande quantidade nesse dia.

O gráfico geral do período registrou média de 1.890 b/s e ponto de mínimo de 394,67 bps para o tráfego de entrada. Para o tráfego de saída, foi registrada média de 2.530 bps e ponto de máximo de 121.260 bps.

Apesar de, ao se olhar o gráfico geral do período, o ponto de máximo da variável *traffic_in* parecer ter sido registrado no dia 07/12 (quarta-feira), tal ponto foi registrado no dia 10/12 (sábado), cujo gráfico está representado na figura 56, e é de pouco mais de 170.000 bps (considerando-se que a diferença entre cada valor do gráfico é de 50.000 e há cinco

quadriculados entre cada valor, o que faz cada quadriculado ter valor de 10.000).

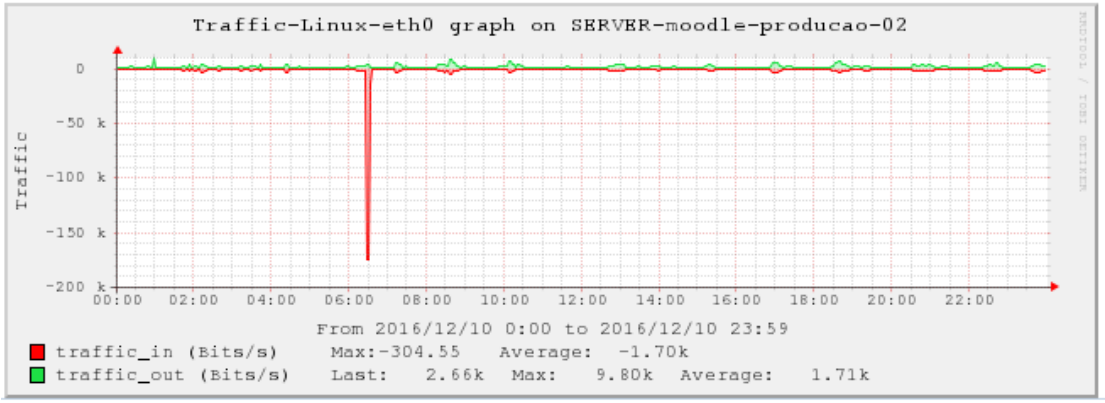

Figura 56 – Gráfico de tráfego do servidor do Moodle relativo ao dia 10/12.

5.2. Servidor de testes do Moodle

Para a análise do servidor de testes do Moodle, foi escolhido o período entre os dias 06/12 (primeiro dia em que o gráfico esteve disponível) e 10/12. O gráfico para esse período é mostrado na figura 57.

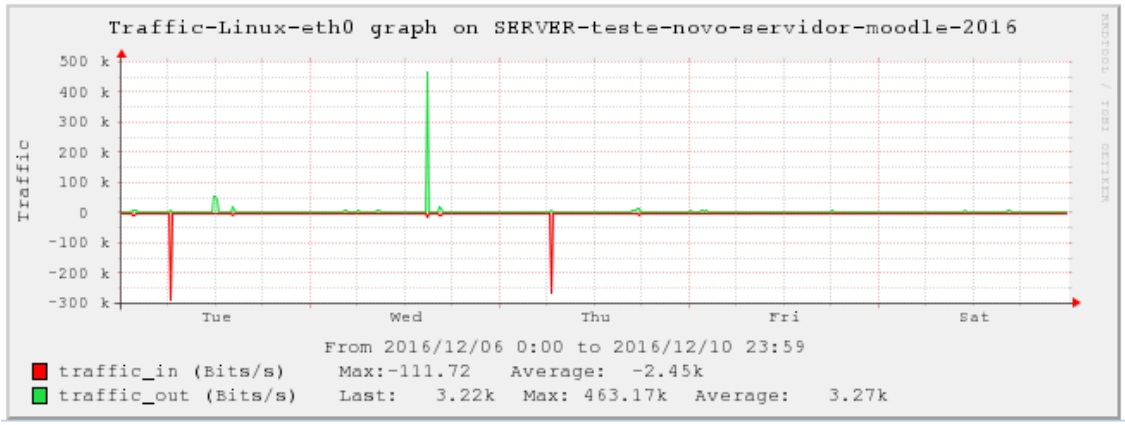

Figura 57 – Gráfico de tráfego do servidor de testes do Moodle.

Pode-se perceber que o tráfego ficou praticamente zerado fora dos momentos de maior quantidade. Por sua vez, esses momentos indicaram valores bem maiores que os do servidor oficial do Moodle, o que possivelmente foi originado por testes de estresse em que foram feitos uploads e downloads em massa.

O gráfico geral do período registrou uma média de 2.450 bps para a variável *traffic_in*, com ponto de mínimo de 394,67 bps e ponto de máximo de aproximadamente 300.000 bps.

Para a variável *traffic_out*, foi registrada uma média de 3.270 bps, com ponto de máximo de 463.170 bps.

O ponto de máximo da variável *traffic_in* foi registrado no dia 06/12 (terça-feira), cujo gráfico é mostrado na figura 58. Pelo gráfico desse dia, o ponto de máximo é, na verdade, de aproximadamente 500.000 bps.

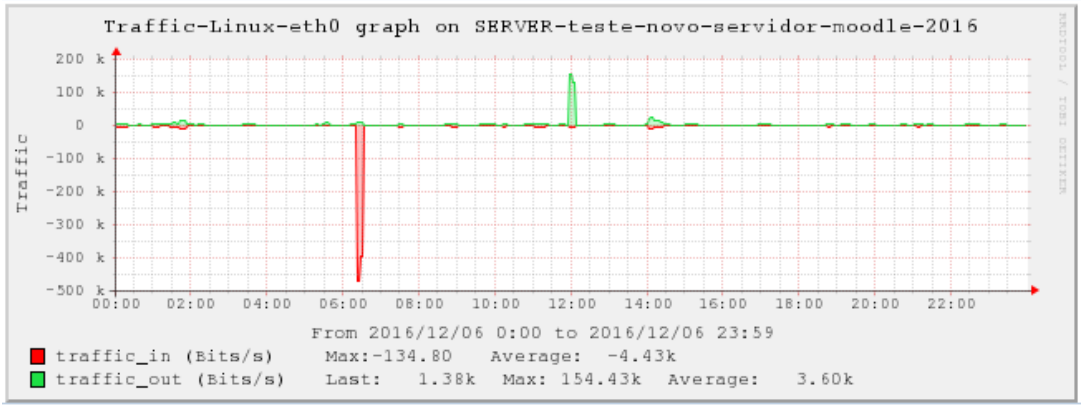

Figura 58 – Gráfico de tráfego do servidor de testes do Moodle relativo ao dia 06/12.

5.3. Servidor do SAT (sistema de abertura de chamados)

Para a análise do servidor do SAT foi escolhido o período entre os dias 06/12 (primeiro dia em que o gráfico esteve disponível) e 10/12. O gráfico para esse período é mostrado na figura 59.

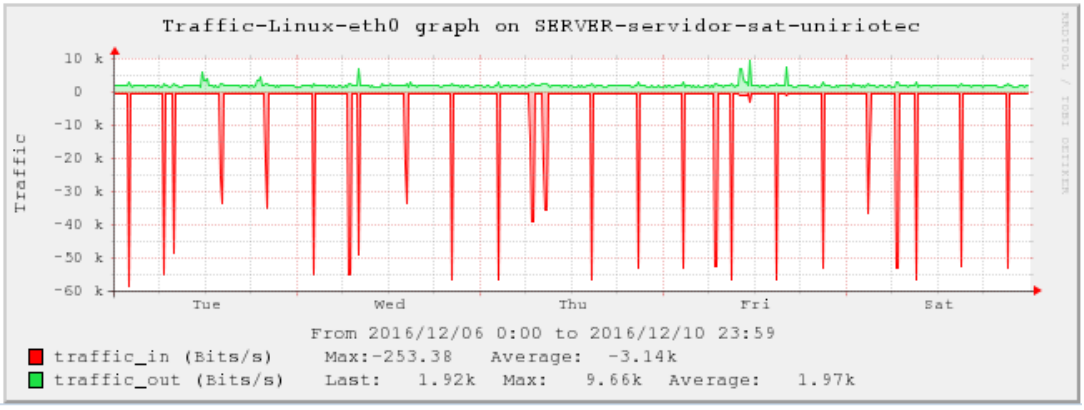

Figura 59 – Gráfico de tráfego do servidor do SAT.

A imensa discrepância entre a quantidade de tráfego de entrada e a quantidade de tráfego de saída, conjuntamente ao fato de que um sistema de abertura de chamados tende a

possuir uma frequência maior de chamados abertos que de chamados atendidos para um dado período de tempo, mostra que o sistema recebeu uma grande quantidade muito grande de chamados neste período.

O gráfico geral do período registrou uma média de 3.140 bps para a variável *traffic_in*, com ponto de mínimo de 253,38 bps e ponto de máximo de aproximadamente 60.000 bps. Para a variável *traffic_out*, foi registrada uma média de 1,97 bps, com ponto de máximo de 9.660 bps.

Apesar de, ao se olhar o gráfico geral do período, o ponto de máximo da variável *traffic_in* parecer ter sido registrado no dia 06/12 (terça-feira), tal ponto foi registrado no dia 09/12 (sexta-feira), cujo gráfico está representado na figura 60, e é de aproximadamente 150.000 bps.

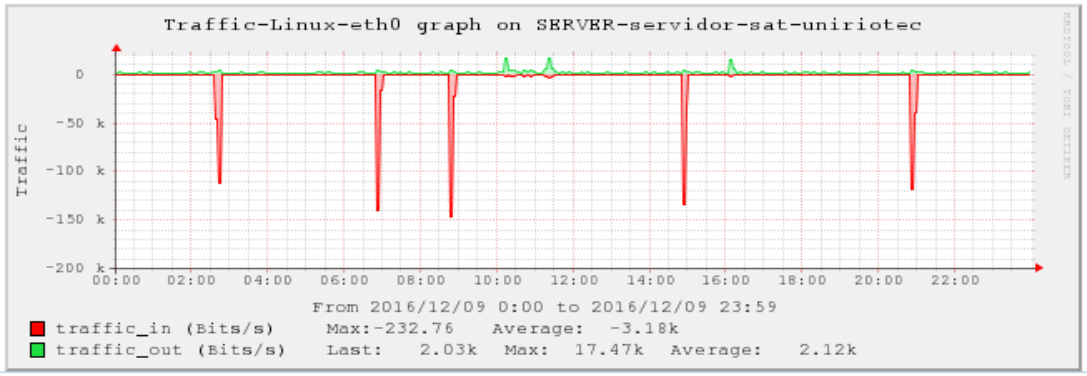

Figura 60 – Gráfico de tráfego do servidor do SAT relativo ao dia 09/12.

5.4. Servidor de hospedagem da página web do portal do BSI

Para a análise do servidor de hospedagem da página web do portal do BSI, foi escolhido o período entre os dias 06/12 (primeiro dia em que o gráfico esteve disponível) e 10/12. O gráfico para esse período é mostrado na figura 61.

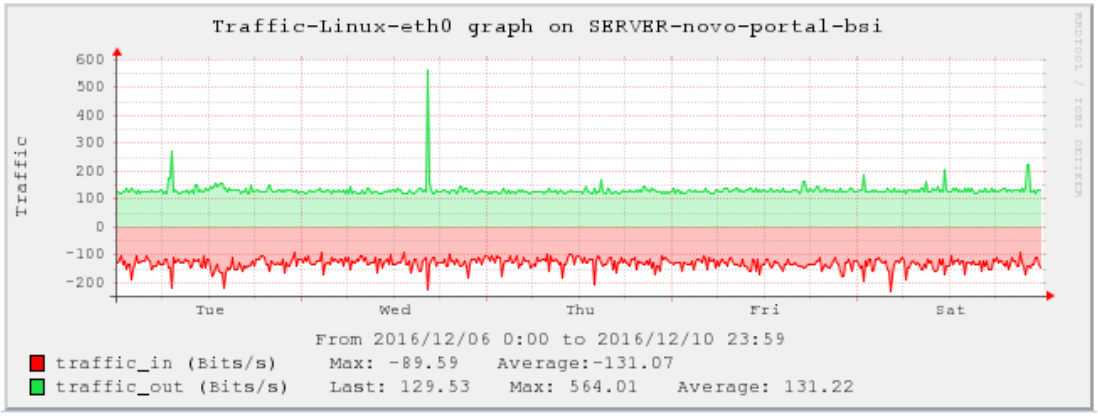

Figura 61 – Gráfico de tráfego do servidor de hospedagem do portal do BSI.

Foi possível verificar que o tráfego de entrada e o tráfego de saída foram praticamente iguais, o que é normal para servidores que hospedam sites, uma vez que o servidor funciona atendendo instantaneamente a requisições que chegam.

No gráfico geral do período, para a variável *traffic_in* foi registrada uma média de 131,07 bps, com ponto de mínimo de 89,59 bps e ponto de máximo de aproximadamente 300 bps. Para a variável *traffic_out*, foi registrada uma média de 131,22 bps, com ponto de máximo de 564,01 bps.

O ponto de máximo da variável *traffic_in* foi registrado no dia 10/12 (sábado), cujo gráfico está representado na figura 62. Pode-se perceber que o ponto de máximo está em conformidade com o gráfico geral.

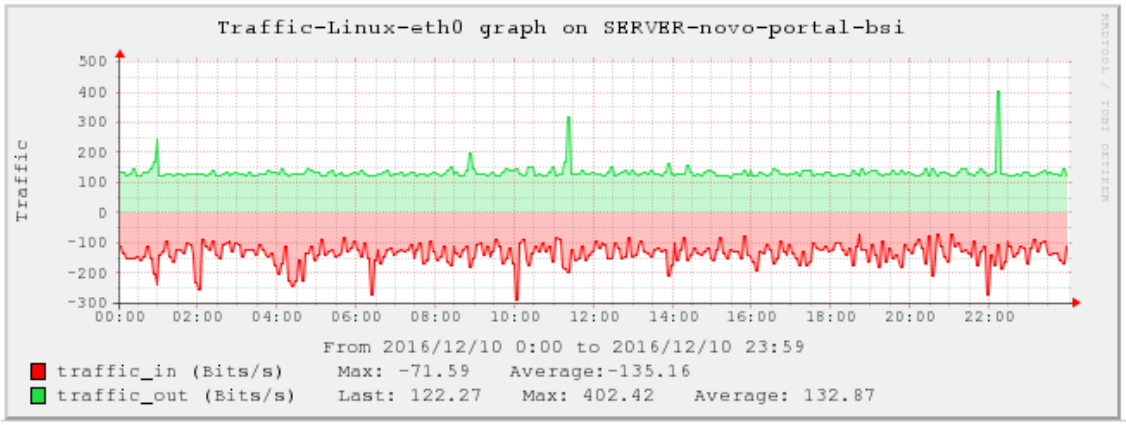

Figura 62 – Gráfico de tráfego do servidor de hospedagem do portal do BSI relativo ao dia 10/12.

5.5. Servidor de backups

Para a análise do servidor de backups, foi escolhido o período entre os dias 06/12 (primeiro dia em que o gráfico esteve disponível) e 10/12. O gráfico para esse período é mostrado na figura 63.

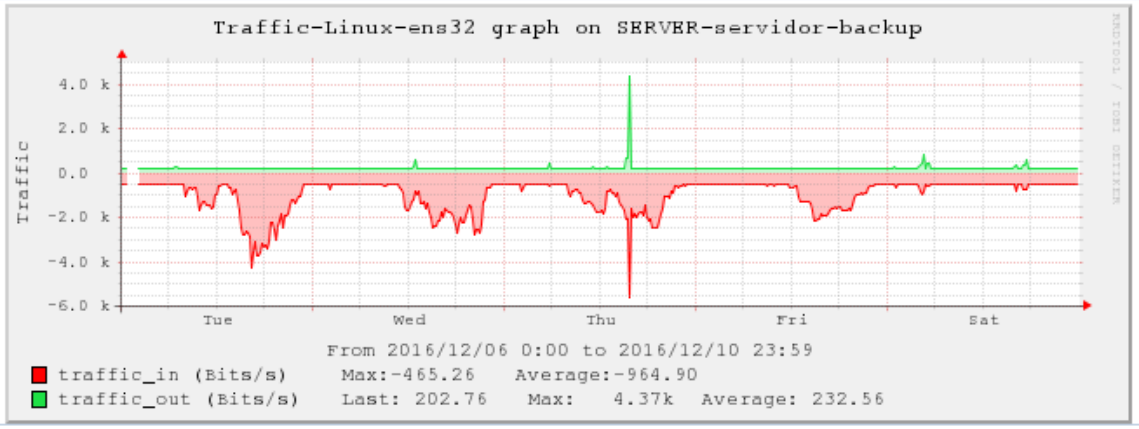

Figura 63 – Gráfico de tráfego do servidor de backups.

Em um servidor desse tipo, é esperado que as operações de gravação dos backups sejam feitas em maior número que as operações de restauração destes, o que, consequentemente, gera um tráfego de entrada muito maior que o tráfego de saída. É exatamente isso o que se vê no gráfico, com picos e momentos de valores altos na casa dos quatro dígitos para o tráfego de entrada.

Para a variável *traffic_in*, foi registrada uma média de 964,90 bps, com ponto de mínimo de 465,26 bps. O ponto de máximo é indicado no gráfico geral do período como sendo de aproximadamente 6000 bps, mas o gráfico do dia 08/12 (figura 64), no qual foi registrado esse ponto, revela que foi, na verdade, de aproximadamente 14.000 bps (considerando que há cinco quadriculados entre cada valor do gráfico e a diferença entre os valores é de 10000, o que faria cada quadriculado possuir valor de 2000).

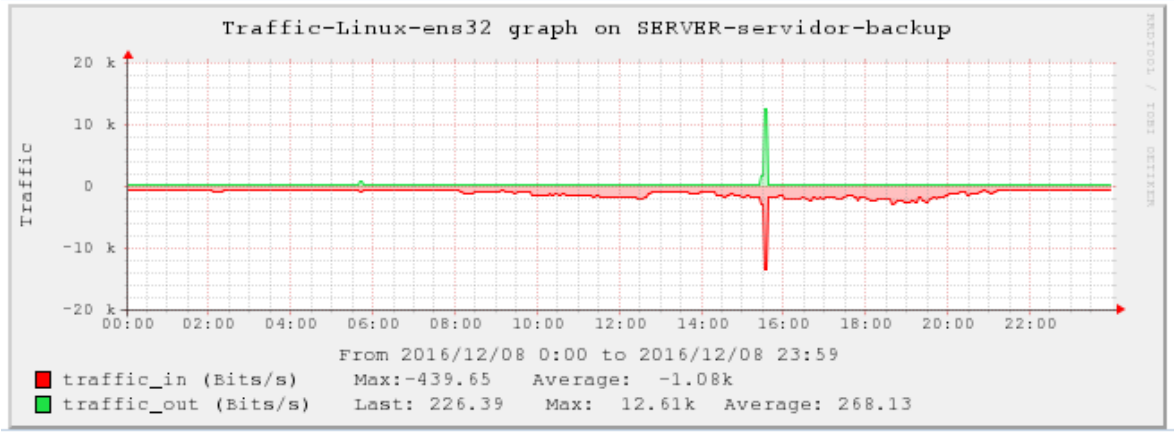

Figura 64 – Gráfico de tráfego do servidor de backups relativo ao dia 08/12.

Para a variável *traffic_out*, o gráfico geral do período registra uma média de 232,56 bps, com ponto de máximo de aproximadamente 4370 bps; porém, o gráfico do dia 08/12 (no qual, assim como no caso da variável *traffic_in*, esse ponto foi registrado) também indica uma quantidade bem maior: Pouco mais de 12000 bps.

O dia 08/12 (quinta-feira) foi o único em que a variável *traffic_out* chegou a um patamar comparável ao da variável *traffic_in*. A causa disso reside, provavelmente, em uma restauração de backup feita paralelamente a uma gravação de backup.

5.6. Avaliação geral da análise

A utilização da funcionalidade de gráficos do Centreon permitiu obter dados mais intrínsecos sobre o tráfego da rede, inclusive evidenciando, em alguns servidores, comportamentos que, embora possuíssem justificativas plausíveis, foram bastante diferentes dos padrões apresentados. Dois exemplos disso foram o servidor do Moodle e o servidor de backup, que tiveram alguns dias com registros de valores bem mais altos que os valores mais comuns mostrados pelas análises. A sinalização destes desvios em relação a um comportamento esperado, seja ela meramente visual ou através de plugins que possam disparar alarmes, permite aos administradores da rede verificarem se estes comportamentos estão relacionados a problemas para os quais seja necessária uma reação ou se é necessário algum replanejamento da rede para melhor acomodar surtos legítimos de tráfego.

Após a análise dos cinco servidores especificados, foi possível concluir que, embora o Centreon tenha demonstrado apresentar algumas inconsistências em seus gráficos, os dados

apresentados foram satisfatórios e condizentes com o que se esperava do comportamento dos servidores, não tendo sido verificados comportamentos anormais – o que é um resultado ainda melhor quando se considera que os servidores monitorados desempenham atividades que estão entre as mais importantes dentro da rede.

6 Conclusão

O presente trabalho, motivado pela necessidade de evolução da política de monitoramento de rede da EIA, objetivou documentar a implantação do sistema de monitoramento Centreon, contendo também detalhes sobre o monitoramento de redes em si, tanto sobre como ele é feito quanto sobre ferramentas que o aplicam. Foi mostrada uma breve história do monitoramento de alguns sistemas de monitoramento via web, dentre eles o Cenreon, que foi o objeto de implantação do presente trabalho e, devido a isso, foi detalhado de forma bem mais intrínseca, com uma documentação precisa sobre sua instalação e sobre uma de suas formas de configuração que atendeu ao propósito deste trabalho.

Futuramente, pode ser aplicada uma atualização de versão do Centreon para, além de manter o sistema o mais próximo possível de sua a versão mais recente, verificar se foram corrigidos os bugs relatados na análise de tráfego de rede. É possível também efetuar testes com outros sistemas de monitoramento via web disponibilizados de forma gratuita, como o OpenNMS, citado no capítulo 3, ou o Zabbix, que é um dos sistemas mais populares atualmente e conta com um grande número de usuários a nível corporativo, além de possuir funcionalidades nativas que o Centreon não possui, como, por exemplo, a geração de mapas de rede.

Outra sugestão de trabalho futuro é realizar implantações de Plugin Packs do Centreon, que fornecem modelos de configurações para vários dispositivos e protocolos. Na infraestrutura da Escola de Informática Aplicada, será possível utilizar estes plugins para monitorar bancos de dados e roteadores, por exemplo.

Referências Bibliográficas

BAUERMANN, D. **Monitoramento de rede de A a Zabbix**. Disponível em: < http://pt.slideshare.net/tchelinux/monitoramento-rede>. Acesso em: 25 jun. 2010.

BENINI, R. A.; DAIBERT, M. S. Monitoramento de redes: trabalhando com a ferramenta Nagios. **Infra Magazine**, n. 1, p. 63, 2011.

BIRCH, S. **The history of network management**: an infographic. Disponível em: <https://www.irisns.com/the-history-of-network-management-an-infographic/>. Acesso em: 12 mar. 2016.

BRAGA, J. O. **Estudo sobre o protocolo SNMP e comparativo entre ferramentas**. 2012. 31 fev. Trabalho de Conclusão de Curso (Especialização) - Faculdade de Ciências Exatas e Tecnológica, Universidade Tuiuti do Paraná, Curitiba, 2012.

CENTREON. Centreon Documentation. Disponível em: <https://documentation.centreon.com/>.

DIAS, H. L. **A importância do monitoramento de ativos de redes**: **um estudo de caso com o sistema CACIC.** 2008. 67 f. Trabalho de Conclusão de Curso (Bacharelado) - Escola Politécnica, Universidade de Pernambuco, Pernambuco, 2008. Disponível em: <http://tcc.ecomp.poli.br/20082/TCC_Henrique_Dias_2008-2.pdf>.

KUROSE, J. F.; ROSS, K. W, **Redes de computadores e a internet: uma abordagem Top-Down**. 5. ed. São Paulo: Pearson, 2010.

MAURO, D. R.; SCHMIDT, K. J. **SNMP Essencial**. 2nd ed. Sebastopol, CA: O'Reilly Media, 2005.

MICROSOFT. **How SNMP works.** Updated: March 28, 2003. Disponível em: < https://technet.microsoft.com/en-us/library/cc783142(v=ws.10).aspx >.

OLIVEIRA, D. T. **Gerência de redes de computadores**: **uma abordagem com o uso do SNMP.** 2002. 85 f. Trabalho de Conclusão de Curso (Bacharelado) - Ciência da Computação,Centro Universitário do Triângulo (Unitri), Uberlândia, 2008. Disponível em: <http://www.computacao.unitri.edu.br/downloads/monografia/28211129405651.pdf>.

BRISA (Sociedade Brasileira para Interconexão de Sistemas Abertos). **Gerenciamento de Redes- Uma abordagem de Sistemas Abertos.** Makron Books do Brasil, 1993.

FANG, K.; LEIWARD, A. **Network Mangement - A Practical Perspective.** Addison-Wesley Publishing Company, 1993.

ROSE, M. **The Simple Book: An Introduction to Management of TCP-IP based Internets.** Englewood Cliffs, 1995

RIBEIRO, C. E. F. **Centreon, Monitoramento de ativos de rede.** FAME Treinamentos, 2015. Curso online. Disponível em < http://udemy.com >.

VASSALLO, D. **Troubleshooting Centreon graphs.** Acesso em: 26 mar. 2017. Disponivel em: < http://blog.davidvassallo.me/2012/02/17/troubleshooting-centreon-graphs/ > .

YU, J. **Round Robin Databases.** Acesso em: 28 mar. 2017. Disponivel em < https://jawnsy.wordpress.com/2010/01/08/round-robin-databases/ >.