Final

Desenho e Implementação de uma Plataforma Integrada para Monitorização e Gestão da Rede da UMa

PROJETO DE MESTRADO

Rui Pedro Rocha Ruel
MESTRADO EM ENGENHARIA INFORMÁTICA

UNIVERSIDADE da MADEIRA
A Nossa Universidade
www.uma.pt

fevereiro | 2016

Desenho e Implementação de uma Plataforma Integrada para Monitorização e Gestão da Rede da UMa

PROJETO DE MESTRADO

Rui Pedro Rocha Ruel

MESTRADO EM ENGENHARIA INFORMÁTICA

ORIENTADORA

Lina Maria Pestana Leão de Brito

CO-ORIENTADOR

Eduardo Miguel Dias Marques

Resumo

Na atualidade, as estruturas e serviços de redes informáticas massificaram-se de forma heterogénea. Aumenta, assim, a importância de garantir aos utilizadores, segurança, fiabilidade e disponibilidade da rede. Posto isto, os administradores de redes têm de manter uma qualidade de serviço elevada utilizando novas formas de vigiar a rede.

No âmbito deste projeto, o trabalho desenvolvido, atendendo às necessidades principais do ambiente a ser monitorizado, pretende-se implementar uma solução integrada de gestão das Tecnologias de Informação da Universidade da Madeira, para permitir uma gestão preventiva e corretiva.

A abordagem selecionada começou com a fundamentação e conceitos teóricos sobre a gestão de rede, apresentando modelos de gestão de redes e o estudo de quatro sistemas, de domínio público, de gestão e monitorização de redes, destacando as suas principais arquiteturas e funcionalidades.

O trabalho continuou com a contextualização do problema através do estudo e descrição da dimensão e da heterogeneidade da rede da Universidade da Madeira. Prosseguiu com a criação de vários cenários de rede que serão utilizados ao longo do trabalho, como apoio nas três partes em que este foi dividido para obter a solução pretendida, nomeadamente a “Contextualização do problema”, “Análise e Desenho da solução” e “Implementação da solução”.

Na criação de uma arquitetura de uma solução, tendo em conta as prioridades definidas pelo gestor de rede, este trabalho fornece à Universidade da Madeira um sistema de monitorização e gestão integrada, através do qual os seus gestores de rede poderão, de forma eficiente e contínua, gerir as Tecnologias de Informação pertencentes a esta Instituição.

Palavras-chave: Universidade da Madeira, gestão e monitorização de redes, ferramentas de gestão, solução integrada de gestão, Tecnologias de Informação.

Abstract

Currently, computer structures and networking services are expanding heterogeneously. Thus increasing the need to provide users with safety, reliability and network availability. As such, network administrators have to maintain a high quality of service using new ways to monitor the network.

Under this project, the work, taking into account environmental main needs to be monitored, an integrated management solution of Information Technologies at the University of Madeira has been implemented to allow for preventive and corrective management.

The selected approach began with the foundation and theoretical concepts of network management, featuring network management models and the study of four public domain network monitoring and management systems, while highlighting the main architectures and features.

The work proceeded by contextualizing the problem through the study and description of the size and heterogeneity of the university's network. It continued with the creation of various network scenarios that will be used throughout the work, as a support in all three parts in which it was divided to obtain the required solution, namely "Context of the problem", "Analysis and Design of the solution" and "Implementation of the solution."

Considering the priorities set by the network manager, this work provides the University of Madeira with a monitoring and integrated management system. Through it, their network managers can efficiently and continuously, manage the Information Technologies of the institution.

Keywords: University of Madeira, management and monitoring of networks, management tools, integrated management solution, Information Technologies.

Agradecimentos

Nunca fui um Homem de grandes palavras, mas certamente que não prescindirei de agradecer aos inúmeros intervenientes, que participaram não só no meu projeto de mestrado como em todo o meu percurso académico e pessoal, que certamente sozinho não o teria alcançado. Sei que não à uma enumeração específica que faça este agradecimento mais ou menos justo, fazendo-o assim da forma mais genuína possível.

- Agradeço às pessoas mais importantes da minha vida, os meus pais, que sempre e incondicionalmente apoiaram-me, fazendo-me acreditar que era capaz de atingir tudo o que quisesse por maiores que fossem as adversidades, sem desistir, persistindo nos meus objetivos com foco e determinação sem nunca perder a serenidade. No decorrer deste meu projeto lidei com severas adversidades da vida, podendo no entanto constatar que a força e a determinação que os meus pais sempre demonstraram é possível e verdadeira. Continuo hoje e sempre a sentir a presença vital da minha mãe, pois sinto que por mais longe que estejamos ela estará sempre comigo.

- Agradeço à minha orientadora Prof. Dr.ª. Lina Brito e ao meu co-orientador Prof. Dr. Eduardo Marques pelo apoio, transmissão de conhecimentos, orientação, motivação, disponibilidade e compreensão nos momentos menos bons no percorrer deste projeto. Agradeço especialmente à minha orientadora, pela iniciativa de me propor este projeto de mestrado, que desde o início para mim é muito interessante.

- Agradeço ao Gestor de Rede da Universidade da Madeira o Dr. Gilberto, pela sua disponibilidade que sempre demonstrou, inicialmente no levantamento de requisitos e nas necessidades da rede, e no apoio ao longo da realização deste projeto.

- Agradeço à minha Princesa Jéssica Freitas, que antes de ser minha namorada é a minha melhor amiga, pela sua paciência e persistência, que contribuíram para a conclusão deste projeto. Pelas suas palavras meigas e confortantes. Por acreditar sempre em mim nos momentos mais difíceis. Pelo amor, carinho, compreensão e força que me deu e transmitiu nas turbulências da vida que aconteceram durante o percurso universitário. Pela sua inteira disponibilidade e apoio que sempre demonstrou durante a realização deste projeto.

- Agradeço ao meu padrinho Juan Rodrigues, que como um verdadeiro amigo sempre apoio-me em múltiplos aspetos da minha vida, e concretamente no percorrer deste projeto, estando sempre disponível para me ajudar.

- Agradeço ao meu irmão Hélder Ruel, aos meus avós, tios e tias, primos e primas, cunhadas, sogros e Maria Inês pela preocupação e apoio sempre. Agradeço especialmente aos meus sobrinhos Tomé, Salvador, Santiago, Pedro e Isabel por me fazerem sorrir, contribuindo nos momentos de maior *stress*.

- Agradeço ao meu amigo Daniel Aguiar e à sua família que desde à muitos anos acompanha-me no meu percurso académico e pessoal. Agradeço especialmente aos meus amigos Nídia Springer e Ricardo Gonçalves pela amizade, apoio e diversão que fizeram sentir sempre que precisei. Agradeço particularmente à Tatiana Severim e ao João Serina pela amizade e inteira disponibilidade que demonstraram para comigo. Agradeço igualmente a todos os meus amigos que direta ou indiretamente fazem parte da minha vida.

- Agradeço aos meus amigos de Campo de Trabalho que muito me ensinaram e apoiaram, agradecendo particularmente à Maria José Moreira pela inteira disponibilidade e aos irmãos Nélio Teles e Susana Teles pelo apoio, motivação e incentivo.

- Agradeço ao Departamento de Informática e Comunicações do Instituto de Emprego da Madeira, nomeadamente ao Engenheiro Xavier Nunes, Emanuel Gonçalves e Rui Bettencourt pelo apoio, incentivo e compreensão para a conclusão deste projeto.

Por último agradeço a todos que diretamente ou indiretamente contribuíram para a concretização deste projeto.

A todos o meu Muito Obrigado!

Índice

Índice de Figuras

Índice de Tabelas

Acrónimos

APs	***A**ccess **P**oints*
ASN.1	***A**bstract **S**yntax **N**otation One*
bps	***b**it **p**er **s**econd*
CPU	***C**entral **P**rocessing **U**nit*
DNS	***D**omain **N**ame **S**ystem*
FCAPS	***F**ault **C**onfiguration **A**ccounting **P**erformance **S**ecurity*
FTP	***F**ile **T**ransfer **P**rotocol*
Gbps	***G**igabit **p**er **s**econd*
HTTP	***H**yper**T**ext **T**ransfer **P**rotocol*
IANA	***I**nternet **A**ssigned **N**umbers **A**uthority*
ICMP	***I**nternet **C**ontrol **M**essage **P**rotocol*
IETF	***I**nternet **E**ngineering **T**ask **F**orce*
IP	***I**nternet **P**rotocol*
ISO	***I**nternational **O**rganization for **S**tandardization*
LDAP	***L**ightweight **D**irectory **A**ccess **P**rotocol*
Mbps	***M**egabit **p**er **s**econd*
Mhz	***M**ega**h**ert**z***
MIB	***M**anagement **I**nformation **B**ase*
OID	***O**bject **Id**entifier*
OSI	***O**pen **S**ystem **I**nterconnection*
PDU	***P**rotocol **D**ata **U**nits*
RADIUS	***R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice*
RAM	***R**andom **A**ccess **M**emory*
RFC	***R**equest **F**or **C**omments*
SASUMa	***S**erviço da **A**ção **S**ocial da **U**niversidade da **Ma**deira*
SMI	***S**tructure of **M**anagements **I**nformation*
SMS	***S**hort **M**essage **S**ervice*
SMTP	***S**imple **M**ail **T**ransfer **P**rotocol*
SNMP	***S**imple **N**etwork **M**anagement **P**rotocol*
SO	***S**istema **O**perativo*
SSH	***S**ecure **Sh**ell*
SSL	***S**ecure **S**ockets **L**ayer*
TCP	***T**ransmission **C**ontrol **P**rotocol*
TI	***T**ecnologias de **I**nformação*
UI	***U**ser **I**nterface*
UMa	***U**niversidade da **Ma**deira*
UTP	***U**nshielded **T**wisted **P**airs*
VLAN	***V**irtual **L**ocal **A**rea **N**etwork*
VM	***V**irtual **M**achine*

Capítulo 1- Introdução

Os sistemas em rede são, atualmente, cada vez mais importantes nas instituições. A evolução das redes de comunicação fez com que tenha crescido de maneira significativa a utilização destes sistemas por parte das organizações. Nesta área, com o aumento exponencial dos serviços em rede, crescem igualmente os serviços suportados pelas redes e, consequentemente, aumentará a necessidade de manter os sistemas em pleno funcionamento ao longo do tempo.

Uma estrutura de rede é composta por um grande ou pequeno número de componentes ativos, tais como, *switches, routers, firewalls, access points*, servidores, e outros, que em conjunto com componentes passivos, tais como, bastidores, cabos, condutas, e outros, formam o alicerce para o funcionamento das diversas aplicações e serviços de rede. Esta estrutura e os serviços básicos, tais como, *Domain Name System* (DNS), *Dynamic Host Configuration Protocol* (DHCP) e a autenticação de utilizadores, são determinantes para a eficácia dos serviços e aplicações de rede, que permitem as empresas ou organizações realizarem as suas funções [1].

Atualmente, as redes caracterizam-se pelo grande dinamismo no que diz respeito ao número, tipos de utilizadores, serviços e aplicações em rede. Os utilizadores pertencentes a instituições, tais como, empresas de grande dimensão, organismos governamentais, instituições de investigação e de ensino, como é o caso da Universidade da Madeira, são consumidores e geradores de um enorme volume de tráfego, dependendo de forma crítica da disponibilidade da rede.

Um administrador de rede nunca poderá estar em descanso. Uma falha de um equipamento poderá ocorrer a qualquer momento. Pode ser necessário alterações de configuração, quer como resposta a alterações de *software* ou de equipamentos, quer na otimização do funcionamento da rede. Para um bom desempenho da rede, essencialmente, devem ser identificados situações anómalas ou estrangulamentos. A segurança da rede também deve ser constantemente assegurada através de mecanismos de autenticação que garantam que o utilizador é quem diz ser e dispor de um controlo de acesso aos serviços, garantindo quem é que tem acesso aos serviços e o que tem direito a fazer [1], [2].

Para a monitorização, gestão e medição na rede, um administrador te de realizar algumas tarefas. Independentemente da dimensão da rede, a sua execução é importante. Algumas tarefas passam por: Verificar periodicamente a conectividade IP dos equipamentos da infraestrutura de rede; Verificar a operacionalidade e medir o desempenho dos serviços de rede; Analisar o tráfego de rede para conhecer os protocolos que estão a ser utilizados na rede; Medir parâmetros de rede, tais como, latência da rede, disponibilidade, perda de pacotes, e outros; Detetar intrusões; Dar suporte técnico; entre outras.

Com o passar do tempo, a alta tecnologia na área das redes informáticas e a criação constante de serviços baseados na rede têm vindo a ter um crescimento significativo, acabando por ser extremamente difícil a um administrador de rede a monitorização e o controlo de uma rede com centenas, ou mesmo milhares, de equipamentos ativos, utilizando apenas técnicas tradicionais para executar as tarefas descritas acima. Estas envolvem a ou deslocação aos equipamentos para verificar o seu correto funcionamento, ou a execução manual de *scripts*, comandos, tais como, *ping* para testar a conectividade IP entre equipamentos através do envio de pacotes ICMP, *traceroute* para verificar rotas entre equipamentos*, netstat* para visualizar o estado das ligações de rede de um equipamento e estatísticas das interfaces, *nmap* para identificar equipamentos e/ou serviços ativos na rede, entre outros, para a verificação da operacionalidade e/ou diagnosticar anomalias na infraestrutura e serviços de rede.

Com base nas dificuldades acima descritas, relativamente à administração da rede através de técnicas tradicionais, torna-se necessário a automatização de muitas destas tarefas, como: a geração e transmissão de vários tipos de alarmes, com diferentes níveis de gravidade; o registo das intervenções para a correção de problemas futuros; visualização gráfica das medições, num determinado período de tempo; e outros. Consequentemente, começaram a surgir no mercado de *software* ferramentas de monitorização e gestão de rede que constituem um elemento importante de suporte para o controlo de todos os recursos de *hardware* e *software* existentes na rede, *a* despistagem de avarias, análises de desempenho, disponibilidade e planeamento.

Estas ferramentas têm como objetivo unificar a monitorização constante de todos os equipamentos de rede num único ponto de controlo e tornando os processos e/ou

tarefas de gestão e monitorização mais autónomos. Isto consiste na monitorização da rede, executando automaticamente verificações periódicas aos dispositivos da rede. Os dados que são recolhidos por estas ferramentas, para além da análise em tempo real da rede, permitem igualmente ser utilizados para histórico de ocorrências

Com o aparecimento das ferramentas de gestão e monitorização, surgiu a comercialização das mesmas, com custos elevados, tornando-se inviável para muitas empresas. Devido aos custos elevados destas ferramentas, começaram a surgir no mercado soluções *open source*, com o objetivo de serem desenvolvidas ao nível de uma solução paga. A simplicidade e flexibilidade destas ferramentas tem tornado possível a sua implementação em sistemas heterogéneos, tanto em redes de grande ou pequena dimensão.

A gestão e a monitorização de uma rede com recurso a uma ferramenta converteram-se num fator vital para a eficiência e produtividade de uma empresa, exigindo um controlo sobre qualquer equipamento localizado na rede que seja possível de ser monitorizado. É quase impossível mencionar a área de gestão de redes sem mencionar o campo da monitorização. A gestão de rede centraliza-se na correção e prevenção de situações anómalas, e a monitorização centra-se na deteção, documentação e notificação das ocorrências.

1.1- Problemas

A Universidade da Madeira depara-se, diariamente, com uma rede com milhares de utilizadores com perfil distinto ao nível dos conhecimentos informáticos, na rede com e sem fios. Este ponto será descrito um pouco mais detalhado no Capítulo 3- .

Esta Instituição possui, centenas de equipamentos ativos, entre eles computadores, servidores, *routers*, *switches* entre outros. Nesta rede encontram-se igualmente vários serviços internos, tais como, *DNS*, *LDAP*, *FTP*, *webmail*, serviços de informação de alunos(*Infoalunos)* e dos docentes(*sidoc*), catálogo bibliográfico da Universidade da Madeira(*biuma*),e outros. Este ponto será abordado no Capítulo 3- .

A Universidade da Madeira, com a sua dimensão, conseguirá gerir e saber com antecedência que ocorreu algum problema relacionado com os seus utilizadores, equipamentos de rede e/ou os serviços prestados pela instituição? A não resolução

deste problema poderá provocar aos utilizadores desta instituição a falha no acesso à internet, a falha na comunicação entre os utilizadores e os serviços internos fornecidos pela Universidade da Madeira.

Na sequência de reuniões com o administrador de rede da Universidade da Madeira identificaram-se alguns problemas relativamente à monitorização e gestão da rede.

Atualmente, a tarefa de monitorização na Universidade da Madeira, não é efetuada por um processo automatizado. O administrador de rede efetua todos os dias testes ou verificações manuais, um a um, aos equipamentos e serviços mais importantes e críticos da rede.

Verificou-se que existe nos serviços técnicos da UMa um desconhecimento geral da situação da rede, nomeadamente, o estado de todos os dispositivos da rede, a quantidade de tráfego presente nas ligações do *backbone* e entre as várias *Virtual Local Area Network* (VLAN) da rede UMa. Ainda, a falta de monitorização de muitos outros aspetos, tais como, a provável sobrecarga de tráfego, a sobrecarga de processamento e utilização nos limites das memórias dos equipamentos.

Outro aspeto detetado foi a ausência de um sistema automático de alertas, que, primeiramente, identifique um equipamento em sobrecarga ou em erro e avise o administrador. Este facto faz com que o gestor necessite de um tempo indeterminado, por vezes de dias ou até semanas, a detetar o equipamento em falha e que, muito provavelmente, está a prejudicar a rede e a comprometer os serviços prestados pela Instituição.

A existência dos problemas no funcionamento da rede, são essencialmente, apresentados por reclamações dos utilizadores, sobretudo na lentidão da rede sem fios. Presentemente, o gestor de rede não tem conhecimento sobre a taxa de utilização dos pontos de acesso e do seu correto funcionamento.

1.2- Objetivos

Em consequência dos problemas descritos anteriormente, identificou-se como objetivo principal deste projeto, melhorar e simplificar o processo de gestão da rede

da Universidade da Madeira, introduzindo processos automatizados para a monitorização e de gestão dos equipamentos de rede.

Pretende-se com este projeto garantir a integridade de toda a informação e estado da rede da Universidade da Madeira através de uma plataforma de gestão e monitorização a implementar, de modo a que o gestor de rede possa confiar nos dados recolhidos e permita ao administrador conhecer de forma mais atualizada o presente estado da rede e dos seus dispositivos, reduzindo o tempo de deteção, identificação e resolução de problemas.

Para a concretização deste projeto são definidos os seguintes objetivos específicos:

- Definir um sistema de monitorização e alertas, que permita ao gestor identificar rapidamente os problemas surgidos na rede, com um maior foco na rede sem fios;
- Possibilidade de analisar localmente e/ou remotamente através de interface *Web* para permitir que o gestor de rede intervenha antes de ocorrer um problema ou antes de ser percetível pelos utilizadores
- Implementar o sistema de monitorização e alertas numa ferramenta nova, que garanta uma gestão preventiva e que possibilite uma gestão corretiva ao gestor de rede dos diversos equipamentos existentes na Universidade da Madeira.

1.3- Estrutura do documento

Este documento está organizado em sete capítulos estruturados da seguinte forma:

- Capítulo 1 – Introdução. Neste capítulo apresenta-se o tema do projeto, com a identificação dos respetivos problemas existentes na Universidade da Madeira, a definição dos objetivos, e por fim, a estrutura do documento deste projeto.
- Capítulo 2 – Contexto tecnológico. Este capítulo encontra-se organizado por dois subcapítulos. No primeiro, apresenta-se a fundamentação e conceitos teóricos sobre a gestão de rede, expõe-se alguns modelos de gestão, a descrição do protocolo da camada de aplicação *Simple Network Management Protocol* (SNMP), do modelo *Fault*, *Configuration*, *Accounting*, *Performance* e

Security (FCAPS), e das VLANs. E, por fim, estuda-se quatro ferramentas de gestão e monitorização existentes no mercado.

- Capítulo 3 – Contextualização do problema. Neste capítulo faz-se a contextualização do problema na Universidade da Madeira.

  A primeira ação centra-se na descrição dos edifícios da Universidade da Madeira, tendo em conta a forma como estão distribuídos alguns serviços internos, o número de postos de trabalho por edifício, o número e tipos de utilizadores. No subcapítulo seguinte concebe-se e descreve-se seis cenários de rede que serão utilizados como "fio condutor" neste projeto para se poder obter uma perceção da dimensão e ter a noção da estrutura da rede da Universidade da Madeira.

  Por fim, apresenta-se uma metodologia com parâmetros específicos para testar e selecionar a ferramenta de gestão
- Capítulo 4 – Análise e Desenho da solução. Este capítulo dedica-se à apresentação de uma solução de monitorização para cada cenário de rede criado no capítulo 3. Ter-se-á em conta características do modelo FCAPS, nomeadamente a gestão de falhas, gestão de *accounting* e gestão de *performance*. Seguidamente, apresenta-se o subcapítulo da seleção da ferramenta onde será demonstrado a comparação das ferramentas e o resultado para poder prosseguir com a instalação da ferramenta no próximo capítulo, designado por "Implementação da solução".
- Capítulo 5 – Implementação da solução. Apresenta-se um subcapítulo com a arquitetura da solução mostrando métodos e processos, regras e nomenclaturas para a criação dos grupos, *hosts*, *triggers* e alertas, com a intenção de que no futuro seja mais simples a adição dos mesmos. Com base nos parâmetros especificados no fim do capítulo 2, será apresentada ferramenta selecionada. Segue-se a implementação dos cenários descritos e desenhados nos capítulos anteriores, na ferramenta selecionada.
- Capítulo 6 – Testes e resultados da implementação. Neste capítulo demostra-se os testes e os resultados efetuados. Em conformidade com a dimensão da Universidade da Madeira e com o propósito de apresentar resultados mais

concretos, os cenários apresentados serão os determinados pelo gestor de rede como os mais críticos.

- Capítulo 7 - Conclusão e trabalhos futuros. Este capítulo corresponde à súmula deste projeto, destacando as principais ilações retiradas no decorrer deste projeto, bem como apresentando linhas e propostas para trabalhos futuros para complementar o trabalho até agora desenvolvido.

Capítulo 2- Contexto tecnológico

2.1- Gestão de Redes

A gestão de redes pode ser dividida em vários níveis, que vão desde uma simples monitorização de meros elementos de uma rede simples de pequena dimensão até uma grande variedade de sistemas numa rede complexa de grande dimensão, passando pela gestão de serviços e aplicações distribuídas [1].

Uma rede consiste na interação de *hardware* e *software* através dos *links, switches, routers, hosts* e outros dispositivos que estão conectados à rede que utilizam protocolos de ligação para serem coordenados, por exemplo, serviços web. Quando centenas ou milhares destes componentes estão conectados numa organização formando um rede, é normal que alguns componentes ocasionalmente possam funcionar mal, que algum componente possa estar mal configurado, algum recurso seja exaustivamente utilizado, ou simplesmente "pare", por exemplo, um cabo danificado.

O administrador de rede, cuja função é manter a rede em perfeito funcionamento, deve ser capaz de responder aos incidentes e, se possível, evitá-los. Para resolver as situações anómalas, o administrador necessita de ferramentas de gestão e monitorização adequadas.

Nesta secção, examinar-se-á a arquitetura, os protocolos e bases de informação utilizadas para estas tarefas por um administrador de rede.

2.1.1- Modelo de gestão Gestor-Agente

O modelo de gestão de rede Gestor-Agente é conceptualmente idêntica a uma simples analogia organizacional humana onde existe o chefe, as filiais e o idioma para comunicar entre o chefe e as filiais. Na área da gestão de redes há uma terminologia própria para os três componentes da arquitetura: uma entidade gestora (o chefe), dispositivos geridos (filiais) e o protocolo de gestão de rede (idioma) [2].

- **Entidade gestora** *(managing entity)* - é uma aplicação controlada por um humano, em geral com uma interface gráfica, uma implementação centralizada

permitindo a recolha ou exibição de toda a informação sobre a atividade da rede, onde analisa e processa alarmes, permitindo ao gestor de rede controlar todos os dispositivos na rede [1];

- **Dispositivo gerido** (*managed device*) - é um equipamento de rede (inclui o seu software) que está localizado na rede que irá ser gerida. Um dispositivo pode ser *host*, *router*, *bridge*, impressora ou qualquer outro que esteja ligado à rede. Dentro dos dispositivos existe um ou mais objetos geridos (*managed objects*) que, na analogia humana, podem ser os vários departamentos dentro das filiais. Estes objetos geridos correspondem aos componentes de *hardware*, por exemplo, a interface de rede, e os parâmetros de configurações entre *hardware* e *software*. Estes objetos contêm peças de informação sobre eles, que são recolhidas numa MIB *(Management Information Base)*, os valores destas peças de informação estão disponíveis para a entidade gestora. Na analogia humana, a MIB são os dados quantitativos (medidas de atividade, produtividade e orçamento, sendo que o orçamento poderá ser configurável pela entidade gestora) trocados entre a filial e o escritório principal, a MIB será abordada no subcapítulo 2.1.2.2- . Por último, cada dispositivo gerido contém um processo, designado por **agente** de gestão de rede, que comunica com a entidade gestora, executa as ações locais no dispositivo gerido sob o comando e controle da entidade gestora. Na analogia humana, o **agente** é o gerente da filial.
- **Protocolo de gestão de rede** - este é executado entre a entidade gestora e os dispositivos geridos, permitindo à entidade gestora consultar o estado dos dispositivos geridos e, indiretamente, tomar ações através dos seus agentes. Os **agentes** podem usar o protocolo de gestão para informar a entidade gestora de acontecimentos excecionais, por exemplo, falha de componentes ou violação dos limites de desempenho. É importante salientar que o protocolo em si não gere a rede, este somente fornece recursos para o administrador poder geri-la [1] [2].

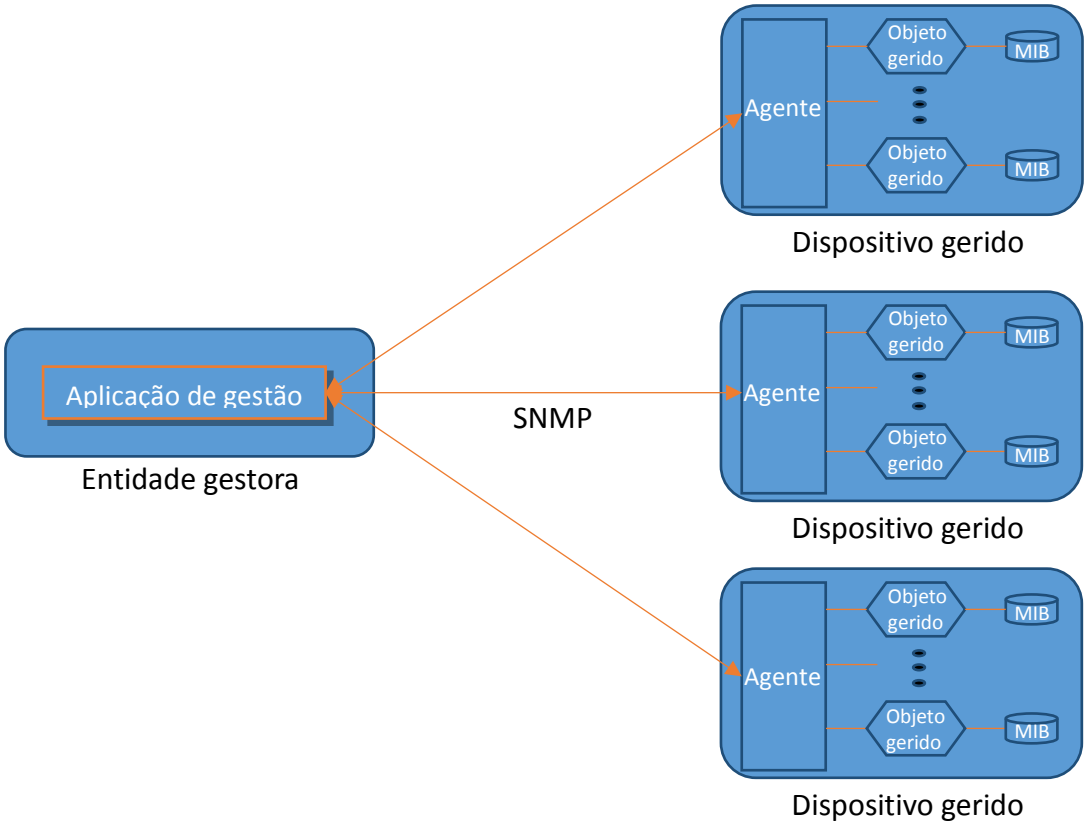


Figura 2.1 – Modelo de gestão Gestor-Agente

2.1.2- Internet-Standard Management Framework SNMP

O *Internet Engineering Task Force* (IETF) propõe uma normalização do modelo de gestão anterior, baseados no paradigma gestor-agente, um pouco mais simples. O *Internet-Standard Management Framework* é designado, geralmente, pelo nome do protocolo de suporte SNMP.

A estrutura do *Internet-Standard Management Framework* é baseada numa arquitetura modular, composta por quatro partes:

- **As definições dos objetos geridos** (*network management objects)* - conhecidos como objetos MIB. A informação de gestão é representada como uma coleção de objetos geridos, em que juntos formam um repositório virtual de informações, denominada por *Management Information Base* (MIB). Concretamente, um objeto gerido pode ser um contador do número de pacotes de entrada e saída numa interface, número de pacotes descartados num *router* devido a erros de cabeçalho, informações descritivas sobre o

dispositivo, por exemplo, versão do *software* de um servidor, informação sobre o seu *status*, e outros;

- **A linguagem de definição de dados** - designado por *Structure of Management Information* (SMI), onde são definidos os tipos de dados, os modelos dos objetos MIB, as regras para a escrita e revisão da informação de gestão;
- **Um Protocolo SNMP** - é usado para comunicar informações e comandos entre a entidade de gestão e agentes;
- **Recursos de segurança e administração** - a adição destes recursos vão, desde uma simples autenticação em comunidade do SNMPv1, até aos mecanismos mais elaborados que são especificados no SNMPv3.

Nos subcapítulos seguintes serão abordados os quatro pontos anteriormente referidos com maior precisão [3] [4].

2.1.2.1- *Structure of Management Information* (SMI)

A SMI é a linguagem usada para a definição das informações de gestão que residem nos módulos MIB. É necessária uma linguagem para garantir que a sintaxe e a semântica dos dados de gestão de rede estão bem definidas e que não permitem ambiguidades. Esta linguagem é baseada na linguagem de definição de objetos *Abstract Syntax Notation One* (ASN.1) da *International Organization for Standardization* (ISO).

A documentação que descreve a versão atual, associada ao SNMPv3, é designada por SMIv2 e está descrita nos *Request for Comments* RFC 2578, 2579 e 2580.

O RFC 2578 define os tipos de dados da linguagem, os tipos de dados básicos estão definidos na Tabela 2.1. A maioria dos tipos de dados são familiares [1], [2], [5], [7].

Tabela 2.1 – Tipos de dados básicos SMI (baseado no RFC 2578)

Tipos de dados	Descrição
Integer	Representa um inteiro definido entre -2^31 e 2^31-1 inclusive, ou um valor de uma lista de possíveis constantes.
Integer32	Representa um inteiro definido entre 2^31 e 2^31-1, inclusive.
Unsigned32	Representa um inteiro definido entre 0 a e^32-1, inclusive.
Octet string	Representa um binário arbitrário ou um texto com limitação de 65535 octetos.
Object identifier	Representa nomes administrativamente atribuídos.
Ipaddress	Representa um endereço IP de 32bits. É representado por 4 octetos (ordem de bytes de rede).
Counter32	Representa um contador de 32bits que incrementa de 0 a 2^32-1 e volta a 0.
Counter64	Representa um contador de 64bits que incrementa de 0 a 2^64-1 e volta a 0.
Gauge32	Representa um número inteiro de 32bits que não faz contagens acima do valor máximo de 2^32-1 nem abaixo do valor mínimo de 0.
Timeticks	Representa o tempo, é medido em centésimos de segundos, decorrido a partir de algum evento.
Opaque	É fornecido apenas para compatibilidade com versões anteriores, este não deve ser usado para tipos de objetos recém-definidos.

Os onze tipos de dados básicos descritos na tabela acima permitem definir os objetos geridos num dispositivo de rede. A Figura 2.2 descreve um objeto na linguagem SMI; neste exemplo, o número total de pacotes que foram entregues com sucesso num dispositivo de rede.

```
ipSystemStatsInDelivers OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
          "The total number of datagrams successfully
          delivered to IPuser-protocols (including ICMP).

          When tracking interface statistics, the counter
          of the interface to which these datagrams were
          addressed is incremented. This interface might
          not be the same as the input interface for
          some of the datagrams.

          Discontinuities in the value of this counter can
          occur at re-initialization of the management
          system, and at other times as indicated by the
          value of ipSystemStatsDiscontinuityTime."
    ::= { ipSystemStatsEntry 18 }
```

Figura 2.2 – Objeto gerido descrito por SMI

2.1.2.2- *Management Information Base* (MIB)

Como descrito anteriormente, a MIB, pode ser interpretada como um repositório virtual de informações, conservando objetos geridos, cujos valores coletivamente refletem o "estado" da rede. Estes valores podem ser consultados e/ou definidos pela entidade gestora, enviando mensagens através do protocolo SNMP para o agente que está no dispositivo gerido.

O IETF ocupa-se da normalização dos módulos MIB associados a *routers, switches* e outros equipamentos de rede, que consiste na identificação base de um determinado *hardware* e a gestão de informações sobre os protocolos e interfaces de rede do dispositivo. Em 2006, existiam mais de 200 módulos MIB normalizados pelo IETF e um número superior de módulos privados produzidos pelos fabricantes dos dispositivos.

Neste contexto, foi necessário a criação de um mecanismo padrão de identificação dos módulos MIB, quer para os módulos já existentes e para os que viessem a ser definidos no futuro. O IETF adotou um sistema de nomeação hierárquico, que já tinha sido posto em prática pela ISO e incluído no ASN.1, que está representado na Figura 2.3, em que cada ponto de ramificação tem um nome e um número, desta forma qualquer ponto da árvore é identificado pela sequência de nomes ou números que especificam desde a raiz até esse ponto.

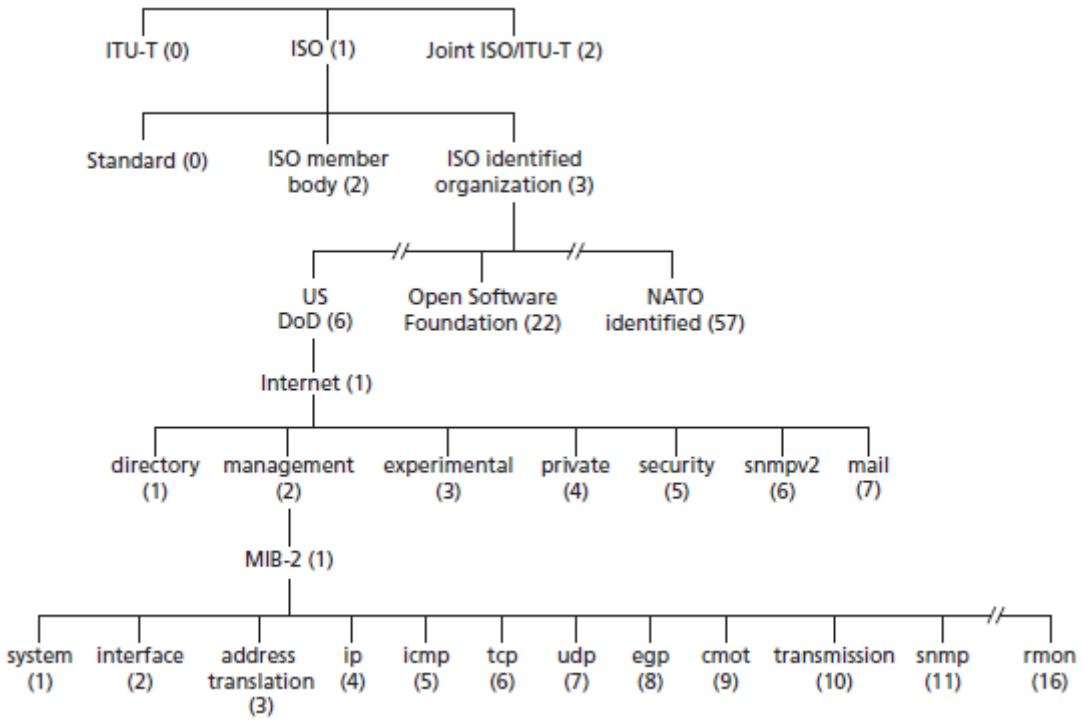


Figura 2.3 – Hierarquia de nomeação de objetos ASN.1

A hierarquia reflete a estrutura de normalização da ISO, ou de normas reconhecidas pela mesma. Sob o ramo *Internet* da árvore (1.3.6.1), existem sete categorias. Sob o ramo *private* (1.3.6.1.4) são reunidos os identificadores privados de todas as organizações privadas que tenham registo com a *Internet Assigned Numbers Authority* (IANA), um exemplo muito conhecido na área das redes é a organização Cisco. Sob o ramo *management* (1.3.6.1.2) e MIB-2 (1.3.6.1.2.1) encontramos as definições padrão dos módulos MIB. Por último, de baixo nível, *system* (1.3.6.1.2.1.1), *interface* (1.3.6.1.2.1.1), encontramos os módulos mais orientados para dispositivos (*hardware)*, assim como os módulos associados aos principais protocolos da internet.

A definição de cada objeto inclui um identificador único, denominado por *Object Identifier* (OID), sob a forma numérica ou legível. Por exemplo, o objeto *interface* acima referido pode ser identificado de duas formas: pelo nome *.iso.isomemberbody.usdod.internet.management.mib-2.interface* ou pelo identificador (1.3.6.1.2.1.1).

O RFC 1213 define a MIB-2, onde são descritos vários objetos geridos, os quais são organizados em grupos. Qualquer dispositivo de rede que suporte SNMP deve reconhecer os objetos geridos da MIB-2. A Tabela 2.2 representa os grupos de objetos geridos, definidos na MIB-2.

Esta tabela foi preenchida com base no RFC 1213 [1], [2], [8].

Tabela 2.2 – Grupos de objetos geridos definidos na MIB-2

Nome	OID	Descrição
System	1.3.6.1.2.1.1	Descrição textual da entidade. Este valor inclui o nome completo e identifica as versões dos sistemas de *hardware*, sistema-operativo e software de rede. Identifica também contacto técnico ou o tempo de decorreu desde que foi iniciado.
Interfaces	1.3.6.1.2.1.2	Mantém informação relativa ao estado das interfaces do dispositivo, tais como, nome e número de interfaces, pacotes enviados e recebidos, erros, etc.
At	1.3.6.1.2.1.3	Sem utilização (deprecated by MIB-2).
Ip	1.3.6.1.2.1.4	Informações sobre o encaminhamento IP, este grupo é obrigatório em todos os sistemas.
Icmp	1.3.6.1.2.1.5	Agrupa informações do protocolo ICMP, este grupo é obrigatório em todos os sistemas.
Tcp	1.3.6.1.2.1.6	Contém informações sobre as ligações TCP.
Udp	1.3.6.1.2.1.7	Informações e estatísticas da utilização do protocolo UDP.
Egp	1.3.6.1.2.1.8	Informações e estatísticas da utilização do protocolo EGP.
Transmission	1.3.6.1.2.1.10	Não contém objetos definidos, é utilizado com base no meio de transmissão subjacente a cada interface, com MIB específicas.
Snmp	1.3.6.1.2.1.11	Inclui informações de desempenho sobre a implementação do SNMP no dispositivo gerido.

Para saber quais são os objetos geridos e onde se localizam na árvore, uma opção seria a leitura dos ficheiros MIB-2 ou, se for o caso, da MIB do fabricante do dispositivo. Uma outra opção, um pouco mais simples, seria a utilização de um MIB *browser* gráfico que auxilia a navegação na MIB. Existem vários produtos deste tipo, uns são comerciais, outros são de utilização livre. Um exemplo que foi útil na realização deste projeto foi a ferramenta de pesquisa disponível em *http://www.oid-info.com* que, através do OID, apresenta informações relativas ao objeto, inclusive uma descrição.

Também igualmente útil na realização deste projeto foi o http://tools.cisco.com/Support/SNMP/do/BrowseOID.do, visto que alguns equipamentos da Universidade da Madeira são equipamentos Cisco.

2.1.2.3- Protocolo SNMP

O *Simple Network Management Protocol* (SNMP), como o próprio nome traduz, é um protocolo de gestão de rede e a denominação mais comum para o ambiente de gestão de redes do IETF é *Internet-Standard Management Framework* que, desde 1990, até à atualidade evoluiu em três versões, sendo na última versão introduzidas funcionalidades de segurança e de controlo de acesso. O protocolo em configuração com um sistema de gestão de rede permite um fluxo de informação variável, fornecendo características e o estado atual (*status),* respondendo aos pedidos ou enviando-lhes notificações sobre situações anómalas entre dispositivos monitorizados e o sistema de gestão que os monitoriza [1] [9].

O SNMPv2 é utilizado para transmitir informações entre as entidades gestoras e os agentes nos dispositivos de rede. A utilização mais comum é o modo *pooling* (pedido-resposta) em que a entidade gestora inicia um pedido para o agente, que recebe a solicitação, realiza uma ação e envia a resposta ao pedido. Este, normalmente é usado para obter (*retrieve*) ou modificar (*set*) valores do objeto MIB do dispositivo gerido. Outro uso comum do SNMP é para o agente enviar uma mensagem não solicitada pela entidade gestora, é designada por trap. Estas mensagens servem para notificar a entidade gestora de uma situação excecional que alterou os valores associados a um objeto, como por exemplo, alteração do estado de uma interface de *Up* para *Down* e vice-versa.

O SNMPv2 define sete tipos de mensagens, conhecidas por *Protocol Data Units* (PDU):

- **GetRequest, GetNextRequest, GetBulkRequest** – estes são enviados de uma entidade gestora para o agente, solicitando um ou um conjunto de valores de um ou mais objetos. Estes três tipos de PDU diferem na granularidade dos pedidos. O *GetRequest* pode solicitar um conjunto arbitrário de valores. O *GetNextRequest* pode ser usado para sequenciar através de uma lista ou

tabela de valores. O *GetBulkRequest* permite que seja devolvido um grande bloco de dados, evitando assim a sobrecarga ocorrida por vários pedidos *GetRequest* e *GetNextRequest*. Em todos este casos o agente responde com uma "PDU Response" que contém os identificadores do objeto e os valores associados,

- **SetResponse** – este é utilizado pela entidade gestora para definir o valor de um ou mais objetos num dispositivo gerido;
- **InformRequest** – este é utilizado pela entidade gestora para notificar outra entidade gestora;
- **Mensagens Trap** – estas são geradas de forma assíncrona, isto é, elas não são geradas em função da resposta a um pedido recebido, mas sim responde a um evento anormal ao qual a entidade gestora exige uma notificação. O RFC 3418 define vários tipos de *Trap*;
- **ResponsePDU** – é utilizado pelo agente para a resposta às mensagens executadas pela entidade gestora.

As mensagens SNMP (*requests e responses*) são transportadas geralmente em pacotes PDU pela porta 161 e, 162 para os *traps*, são permitido outras alternativas.

2.1.3- Modelo FCAPS

Com o crescimento da necessidade de conectar "todos a todos", as funções de gestão de rede aumentaram, as exigências em termos de qualidade de serviço requerida e fornecida aos utilizadores foi alargada a outras áreas funcionais para além de simples falhas. A ISO criou um modelo de gestão de redes onde foram definidos conceitos e modelos informativos para representar recursos, protocolos e informações. Esse modelo é denominado por modelo FCAPS, em que cada letra da sigla representa uma área de gestão. Cada uma destas áreas serão descritas abaixo [10], [11].

- Gestão de Falhas (***F**aults)* – A gestão de falhas trata-se de uma das áreas funcionais mais importantes na gestão de redes, envolvendo quatro etapas: deteção, determinação, diagnóstico e resolução e/ou recuperação. A gestão de falhas recolhe e analisa os alarmes e falhas no serviço. Estas falhas podem ser transitórias ou persistentes. As transitórias não são alarmantes se as

ocorrências não excederem um limiar. No entanto, estes eventos são registados.

As falhas podem ser determinadas a partir de alarmes, em mensagens não solicitadas, ou pela análise a um *log*; esta última analise poderá ser o único recurso quando o serviço ou aplicação não têm a capacidade de vigilância e/ou geração de alarmes internos.

A gestão de falhas analisa e filtra as mensagens de falhas e coordena, de modo, a que o número dos eventos atuais reflita nas condições reais do serviço. Embora todas as falhas são registadas, dependendo da camada, a gestão de falhas poderá resolver. Após a resolução, cria um registo do problema, os seus detalhes e as ações executadas.

A função principal desta gestão é detetar e resolver o mais rápido possível situações que venham a causar um mau funcionamento da rede sem que a mesma pare de estar em produção.

- Gestão de Configuração (***C****onfiguration)* – A configuração de múltiplos serviços é uma tarefa complexa. Uma falha ou um atraso na configuração pode ter um impacto negativo nos serviços prestados aos clientes. A gestão de configuração tem como principal objetivo fornecer a localização, configuração, inventário e manutenção dos agentes em serviço e os seus componentes. As informações sobre os agentes são recolhidas regularmente acompanhado com os tipos de recursos e os seus detalhes. Quando ocorre uma mudança numa configuração de um agente, a gestão de configuração recolhe e analisa as alterações para garantir que estas foram autorizadas e são aceites, as alterações não autorizadas são invertidas e alertadas, pois podem estar a ser alvo de um ataque.

  Esta gestão é responsável pelo ciclo de vida de um serviço desde o início até ao fim. Esta padroniza a ativação e a desativação de serviços de forma regulada e controlada. Também inclui gestão de mudanças para manter o controlo das modificações dos serviços.

  A gestão de configuração é igualmente importante para apoiar as operações de configuração de *transaction-like*, onde vários recursos num ou mais agentes de

serviços podem ser configurados ao mesmo tempo numa única ação. A gestão de configuração mantém todas as versões das últimas configurações efetuadas, permitindo assim a rápida restauração das mesmas. Um componente desta gestão é a ferramenta de descoberta automática de serviços e métodos, que fornece uma descoberta e mapeamento contínuo dos serviços, as suas dependências, componentes e configurações. Esta ferramenta fornece visibilidade precisa, em tempo real, para a configuração de serviços.

- Gestão de Contabilização (***A**ccounting*) – Tem a capacidade de lidar com a especificação dos parâmetros a serem monitorizados em relação à utilização de recursos, estabelecendo limites de uso, monitorizando os custos de utilização, garantindo que as cotas de utilização não sejam excedidas, detetando e relatando a fraude ou tentativas de fraude. Esta gestão também recolhe as informações utilização, analisa a informação e envia relatórios para outros serviços. Igualmente, suporta a auditoria e relatórios de fraude, analisando um suspeito e/ou comportamentos incorretos.

- Gestão de Desempenho (***P**erformance*) – Analisa o desempenho do serviço, recolhe dados de desempenho dos recursos, avalia os dados e emite alertas quando o desempenho real está nos valores dos limites do desempenho. Pode ser capaz de executar medidas corretivas, mantém registos e executa a análise da tendência para poder prever e antecipar problemas de desempenho.
  Esta gestão consiste na definição de políticas de desempenho, medição e sistemas de análise.

- Gestão de Segurança (***S**ecurity*) – Oferece múltiplos serviços de defesa em vários níveis de segurança, controla o acesso e utilização dos serviços, mantem a privacidade, confidencialidade e integridade da informação. Esta gestão é projetada para proteger os serviços e evitar comportamentos maliciosos, negligentes e abusivos por parte dos utilizadores autorizados e não autorizados.

2.1.4- VLAN

As VLAN é um grupo lógico de computadores, servidores e dispositivos de rede, que estão todos na mesma rede física. As VLAN são implementadas com o objetivo de alcançar a escalabilidade, segurança e facilidade em adaptar-se às mudanças nos requisitos de rede e na deslocação de postos de trabalho. [12]

Com o aumento da complexidade das redes informáticas, é comum nos dias de hoje uma rede física ser constituída por várias redes lógicas ajudando na gestão e divisão da rede.[12]

Uma divisão física de uma rede complexa pode-se tornar ineficiente e com custos elevadíssimos. Na análise à figura Figura 2.4, num edifício com imensos pisos, com diversos departamentos distintos, distribuídos pelos andares, em que seja necessário separar todos esses departamentos, será necessário muitos mais *switches* por piso para proceder ao seu isolamento. Num pior cenário, na falta de uma porta em todos os departamentos para conectar um computador de um funcionário de cada departamento específico, seria imprescindível adquirir mais um switch para cada departamento. Estas aquisições provocariam despesas avultadas.

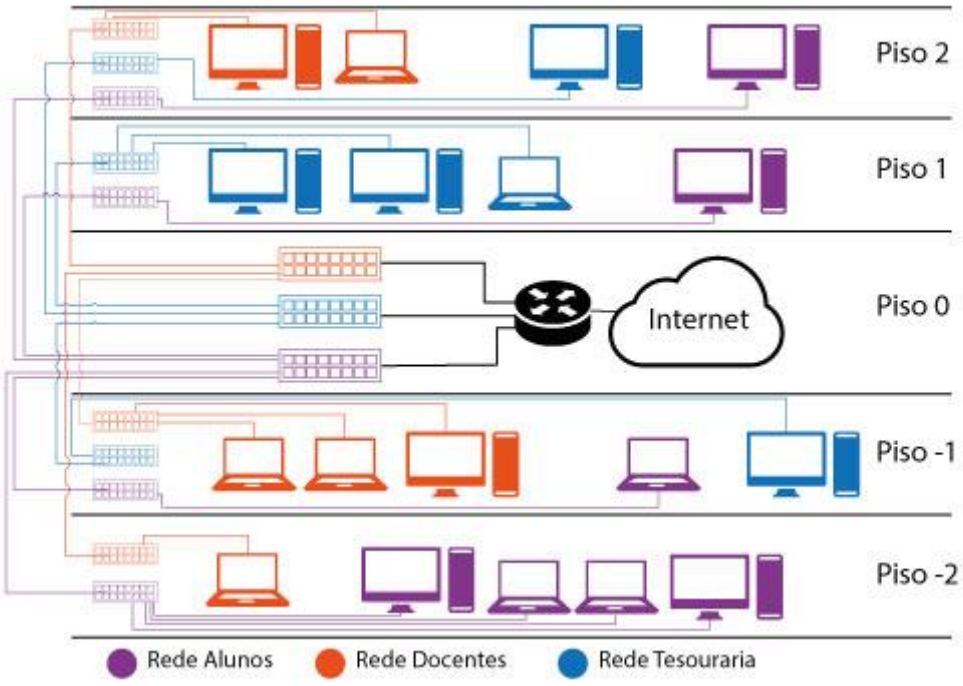


Figura 2.4 – Exemplo de uma rede sem VLANs

A Universidade da Madeira é um excelente exemplo para por em prática estas redes virtuais, VLANs, devido às suas dimensões e utilizadores com perfis distintos, tais como: direção, contabilidade, recursos humanos, alunos, professores, e outros.

É importante que as máquinas estejam em redes lógicas separadas mesmo ligando-se à mesma rede fisica, ao mesmo switch, como é importante que estejam nas mesmas redes logicas ligadas entre switches diferentes. Como por exemplo, por questões de segurança, um aluno não poderá ter acesso à rede dos serviços da contabilidade. A Figura 2.5 ajuda à compreensão desta informação.

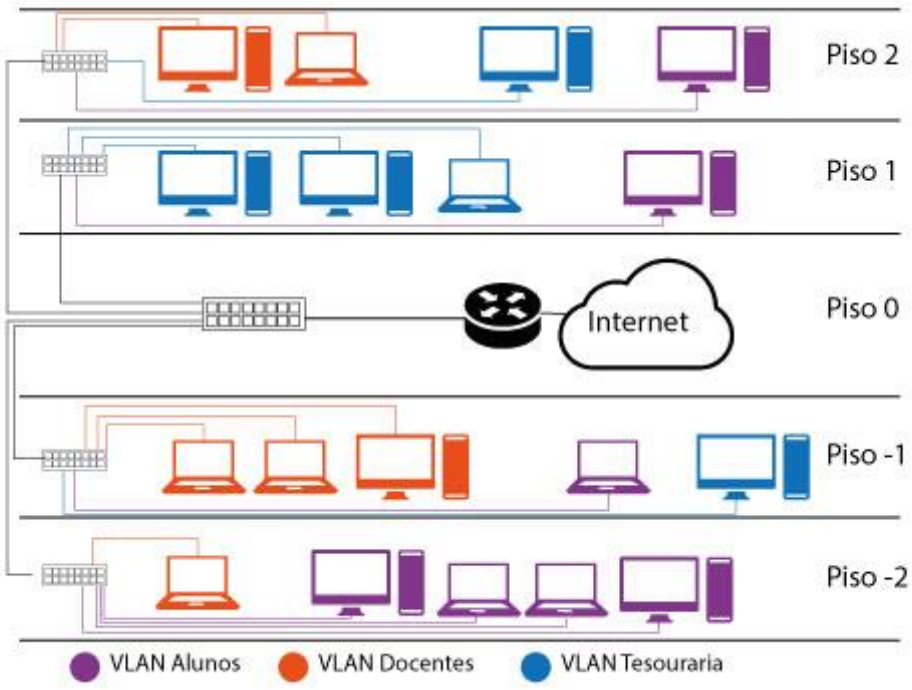


Figura 2.5 – Exemplo de uma rede com VLANs

2.2- IEEE 802.11 (Wi-Fi)

A tecnologia 802.11, é muito famosa na área das comunicações móveis, popularmente conhecida por *Wi-fi*. Atualmente estas redes marcam o dia-a-dia de todos nós porque permitem uma grande mobilidade às aplicações e aos serviços de uma determinada rede. Basta refletir-se na possibilidade de acedermos à internet a partir de um centro comercial, de um café, de um quarto de hotel ou até mesmo no centro de uma cidade sem a sem preocupar-nos com as ligações físicas, por exemplo, cabos.

Para além da mobilidade, as redes sem fios têm outras características importantes, entre as quais, a sua flexibilidade e facilidade na instalação. Estas redes permitem a

possibilidade de projetar uma rede em locais onde seria muito difícil a implementação de uma rede com fios, nomeadamente um edifício histórico que certamente não teria condições para a implementação. Embora, a rede sem fios tenha estas características muito atrativas, nunca deixaremos de ter redes com fios, pois as redes sem fios têm a desvantagem de serem transmitidas por ondas rádio que se degradam com a distância, podem ser absorvidas, refletidas e refratadas e podem ser facilmente bloqueadas por paredes [1], [13].

As redes *Wireless Local Area Network* (WLAN) são definidas no *Standard IEEE* 802.11, são baseadas maioritariamente na utilização de ondas Radio [13]. Uma WLAN geralmente é formada por um ou mais *Access Points* que estabelecem a comunicação entre os dispositivos da rede que permitem a ligação sem fios e o sistema de distribuição, que permite o acesso às aplicações e serviços da rede [13].

As redes sem fios são estruturadas em *Basic Service Set* (BSS) e *Extended Service Set* (ESS). A norma 802.11 explica dois tipos de BSS: independente e infraestruturado [13]. O independente é uma rede *ad-hoc* (ligações diretas entre dispositivos) que não contém *Access Points*. O infraestruturado, é uma ligação entre dispositivos onde existe um *Access Point* que garante todas as comunicações efetuadas entre os dispositivos. A estrutura ESS é composta por vários BSS infraestruturados ligados a um sistema de distribuição para permitir uma cobertura maior da rede sem fios.

2.3- Ferramentas de Gestão e Monitorização de Rede

As ferramentas de gestão de rede é um processo evolutivo e contínuo. Embora as tecnologias de gestão têm vindo a ficar ao longo dos anos mais consistentes, ainda não conseguem atingir o rápido desenvolvimento das redes de computadores. Ainda não existe nenhuma tecnologia que consiga cobrir todo o conteúdo quando confrontado com uma rede extremamente complexa e em constante mudança.

Portanto, a monitorização de rede é uma tarefa exigente, complexa e fundamental, pois muitas organizações dependem da rede para a produção e tomada de decisões.

Contudo, um sistema de gestão de rede é amigo dos administradores, pois este reduz a complexidade das informações de rede em imagens simples, vários tipos de gráficos, tabelas e relatórios sobre a atividade da rede. Permite gerar alertas e ajudar a identificar o tipo de problema, caso exista. Atualmente isto é acessível através de uma plataforma *web*.

Neste projeto será realizada uma análise a quatro ferramentas *open source* do domínio público, descrevendo-as nos subcapítulos seguintes e apresentando as suas arquiteturas e funcionalidades mais evidentes.

2.3.1- Nagios

O Nagios é um sistema de monitorização muito utilizado. Foi criado em 1999 e existem várias versões.

Neste projeto, proceder-se-á a uma análise de duas versões conhecidas desta ferramenta, versão comercial (Nagios XI) e versão open source (Nagios Core)[13].

A versão comercial é uma versão completa e reconhecida na área de gestão de rede. Após a sua aquisição e instalação está apta a monitorizar qualquer tipo de complexidade de rede. A monitorização da rede, de forma visível em tempo real, nas várias formas de gráficos e em tabelas de registos, permite a criação de alertas, de forma, a garantir que os sistemas, aplicações e serviços funcionam corretamente. No caso de uma falha, o Nagios alerta o pessoal técnico da área de redes, o qual permite iniciar os processos de correção, a evitar, muitas vezes, a interrupção total dos serviços da instituição, utilizadores e clientes.

A versão *open source*, denominada por Nagios Core, é idealizada para utilizadores avançados nesta área. Requer a edição dos ficheiros de configuração de forma manual e, numa fase inicial não contém interface gráfico. Possibilita a estes utilizadores o próprio desenvolvimento de extensões, *plugins* e *addons*, e ainda, permite a utilização dos mesmos, programados por terceiros. A partir destes dados verificados, a Nagios começou a criar uma comunidade de programadores externo para desenvolver e disponibilizar na sua página oficial as extensões, *plugins* e *addons*. Presentemente, é

possível, encontrar inúmeras comunidades de programadores em *sites* privados que desenvolvem inúmeras extensões, *plugins* e *addons*, que poderão não ser fiáveis.

Estes processos concebidos permitiu ao Nagios uma expansão da sua flexibilidade e integração de soluções de forma contínua, o que possibilitou complementar ou até substituir vários aspetos da funcionalidade inicial do Nagios, como a interface gráfica, modo de armazenamento de dados ou até o próprio motor de processamento. Desta forma, o Nagios permite construir soluções complexas e completas, dando origem a uma grande semelhança, entre a versão comercial e a versão Core.

O Nagios é baseado num servidor *web* e *Configuration File Options* (CGI). Pode ser integrado com uma base de dados MySQL ou PostreSQL para armazenar as informações para administração. Embora seja recomendado, a base de dados não é essencial para o funcionamento do Nagios. Este pode ser substituído por ficheiros simples, mas esta arquitetura deve ser limitada a pequenas redes com um número limitado de hosts monitorados [13], [14].

A arquitetura padrão do Nagios está representada na Figura seguinte:

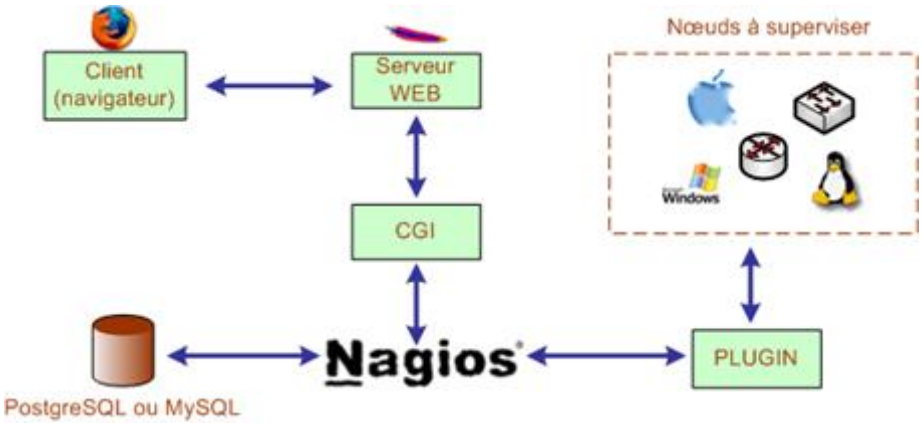


Figura 2.6 – Arquitetura do Nagios

Os *plugins* são programas executáveis ou scripts (*Perl*, *Shell*, e outros) que podem ser executados partir da linha de comandos para testar um *host* ou um serviço. O resultado da execução de um *plugin* é usado pelo Nagios para determinar o estado dos *hosts* e serviços de rede [14].

É possível utilizar agentes para supervisionar e recuperar informações à distância. Estes oferecem a oportunidade de percebermos como os plugins são importantes no Nagios, pois é através dos plugins que estes agentes são criados. Existem dois tipos de agentes mais conhecidos no Nagios:

- Agentes *Nagios Remote Plugin Executor* (NRPE) – O princípio do funcionamento destes agentes é de fácil compreensão. Quando é executado o *plugin* o servidor Nagios inicia a conexão com o agente NRPE ao equipamento a monitorizar, através de um pedido *check_nrpe*, irá permitir ao servidor Nagios obter métricas dos equipamentos como por exemplo, a utilização do disco, carga do CPU, e outros. Seguindo os números da figura abaixo, conseguimos perceber o funcionamento destes agentes [14].

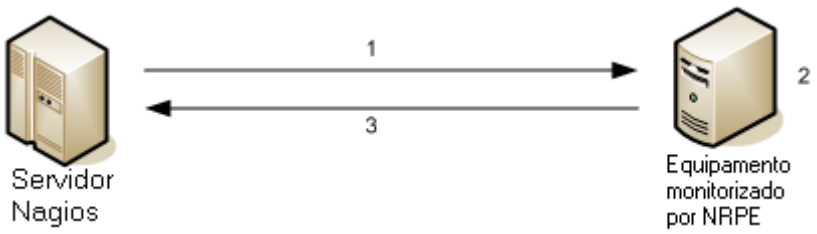


Figura 2.7 – Funcionamento do agente NRPE

- Agentes *Nagios Remote Data Processor* (NRDP) – Diferem dos agentes NRPE, porque a planificação da verificação é executada localmente no equipamento monitorizado e enviado para o servidor Nagios [14].

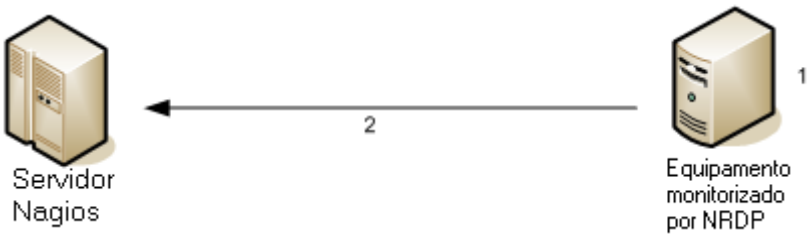


Figura 2.8 – Funcionamento agente NRDP

2.3.2- Icinga

O Icinga é um sistema de monitorização *open source* que surgiu em 2009. Este sistema é muito conhecido por monitorizar inúmeros *hosts* e serviços, notificando o estado dos mesmos aos administradores de rede. O Icinga é um *fork* do Nagios. Tem vindo a merecer relevância e visibilidade ao partilhar semelhanças com o Nagios. No entanto, apresenta algumas diferenças ao nível da arquitetura e ao nível da interface. Quanto à comparação com o Nagios verificou-se um maior grau de agilidade. Em 2012 foi criada uma versão que atualmente permanece em paralelo com a primeira versão, designada por Icinga2, que foi desenhada para poder monitorizar ambientes de grande dimensão e mais complexos. A figura abaixo representa a arquitetura do Icinga [15], [16].

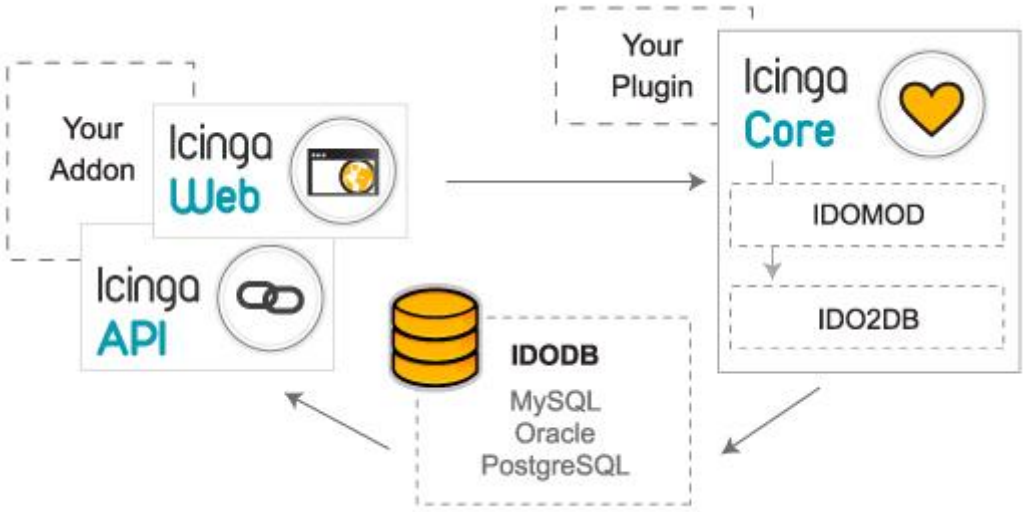


Figura 2.9 – Arquitetura do Icinga

O componente Icinga Core gere as tarefas de monitorização, recebe os resultados das verificações executadas pelos vários plugins, seguidamente comunica esses resultados ao IDODB, através da interface IDOMOD e serviço IDO2DB sobre pacotes *Transmission Control Protocol* (TCP) com encriptação *Secure Sockets Layer* (SSL). A IDODB é a base de dados que é alimentada pelo Icinga Core com as informações dos estados dos *hosts*. Por último, o Icinga Web é a interface *web* para visualizar os resultados da monitorização realizada pelo Icinga Core. Pode-se visualizar o estado dos *hosts*, histórico e notificações para relatar ao administrador o estado da sua rede [17].

O Icinga permite um monitoramento distribuído com recurso a *clusters*. As instâncias dos *clusters*, designadas por satélites, são desenhadas para gerir de forma autónoma e efetuar o equilíbrio das cargas das tarefas de monitorização, notificações e *updates* à base de dados entre eles. Estes também replicam automaticamente configurações, estados dos programas em tempo real e garante a integridade completa dos dados em caso de *Failover* (falha). Toda esta comunicação entre instâncias é assegurada com certificados *x509 SSL*, criando assim zonas de *clusters* seguras [18]. Uma funcionalidade interessante no Icinga é a possibilidade de ter *clusters* que tratam apenas de uma certa tarefa de monitorização, como se pode visualizar na figura abaixo.

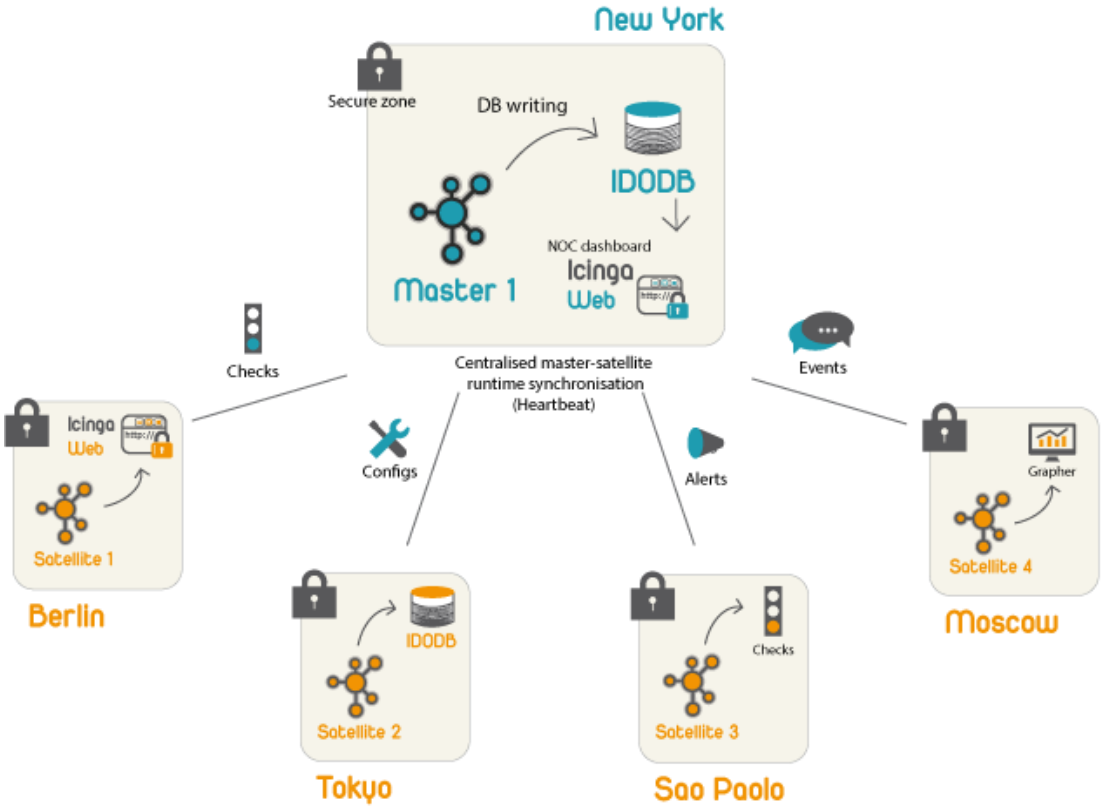


Figura 2.10 – Monitorização baseado em Clusters Icinga

2.3.3- Zenoss

O Zenoss é um *software* de monitorização, criado em 2002 e mantido por uma comunidade de programadores para o aumento de funcionalidades e criação de novos *plugins*. [19]

O Zenoss possui uma arquitetura modular, constituída por quatro camadas.

Pode-se visualizar na figura abaixo [20]:

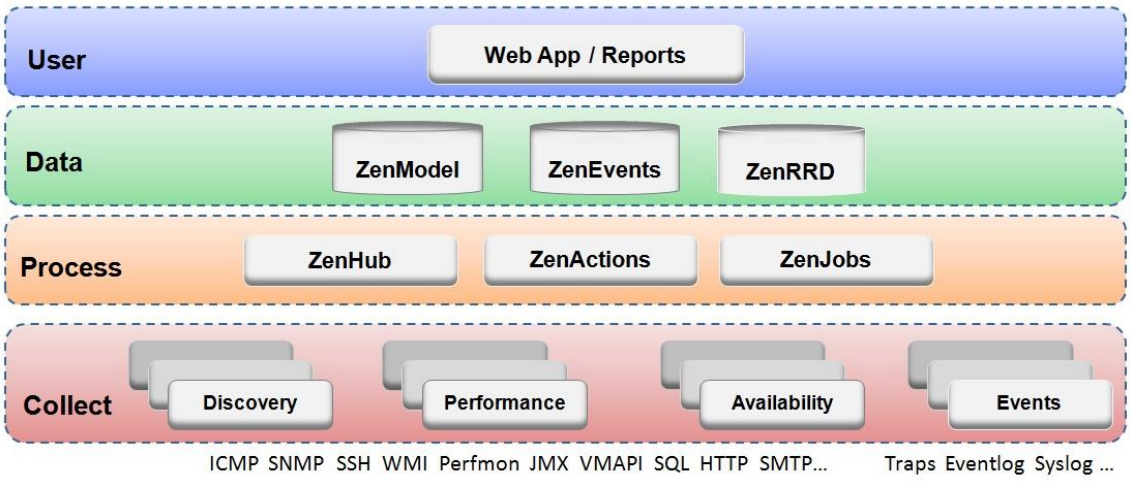


Figura 2.11 - Arquitetura modular Zenoss

Classificadas da seguinte forma:

- Camada da recolha de dados (***Collect***) - esta recolhe os dados dos dispositivos a serem monitorizados usando vários tipos de serviços, entre eles os mais conhecidos SMNP, SSH e WMI, fornecendo as informações à camada de dados. Esta será exposta posteriormente;
- Camada de processamento (***Process***) - esta gera as comunicações entre as camadas adjacentes, utilizando a tecnologia Twisted PB um sistema bideracional do sistema *Remote Procedure Call* (RPC);
- Camada de dados (***Data***) - esta armazena as informações utilizando três repositórios distintos, o ZenModel para configurações, componentes e grupos, o ZenEvents para armazenar dados numa base de dados MySQL e, por último, o ZenRRD para armazenar recolhas de dados temporárias;
- Camada do utilizador (***User***) - onde está presente a interface *web*, onde o administrador pode visualizar o estado dos dispositivos, gerar relatórios, efetuar configurações, e outros. Esta camada foi desenvolvida com base na framework Zope Web, utilizando *JavaScript*.

2.3.4- Zabbix

Zabbix é uma solução de monitorização e gestão de redes, servidores e serviços. É uma ferramenta *open source*, versão *enterprise*, sem custos de licenciamento, pois a sua licença é *GPLv2*.

O Zabbix é uma inovação. As comunidades de utilizadores é um factor importante na resolução de erros e na evolução do sistema Zabbix.

Para a gestão, administração e exibição dos dados recolhidos, esta solução oferece uma interface cem por cento *web* desenvolvida em *php* e *javascript*. O sistema de alertas desta solução pode ser configurado para diversos meios de comunicação, tais como, SMS, *e-mail* e abrir *tickets* em sistemas *helpdesk*. Esta permite igualmente automatismos, isto é, possibilita executar uma ação a um determinado evento de forma automática, como por exemplo, reiniciar um serviço após ter ocorrido um determinado erro.

Esta solução proporciona uma monitorização sem agente (*agenteless*) com suporte a diversos protocolos, conta ainda com descoberta automática de *itens* (*auto-discovery*) e descoberta de métricas nos *itens* que vão ser monitorizados (*low level discovery*).

A figura abaixo descreve o funcionamento do sistema Zabbix entre os componentes.

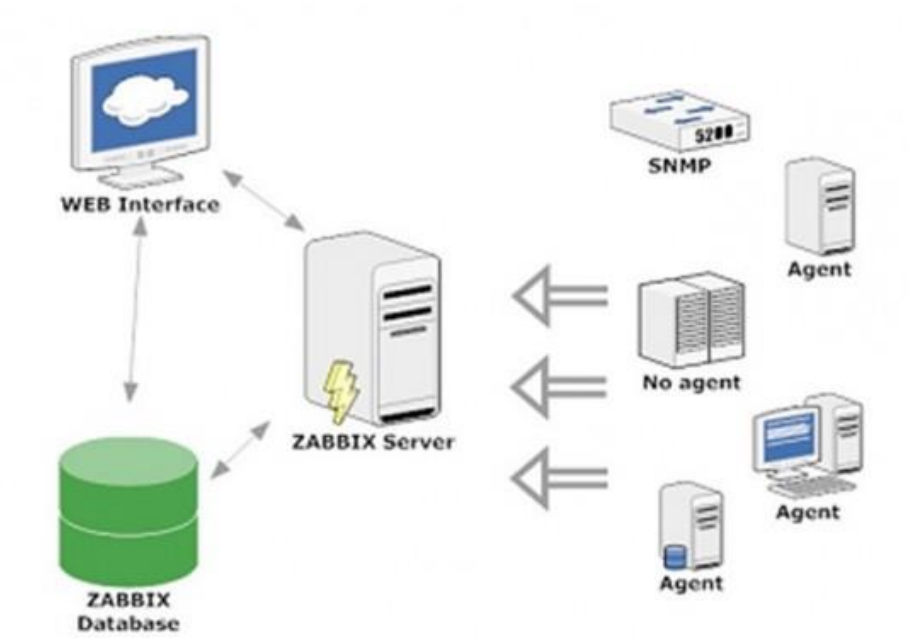


Figura 2.12 – Arquitetura Zabbix

Existem três componentes importantes que serão descritos nos próximos subcapítulos.

2.3.4.1- Zabbix Server

O componente ZabbixServer recolhe os dados necessários para a monitorização sem agentes ou com agentes. Quando é detetada alguma anormalidade na rede, emite alertas através dos sistemas de comunicação existentes, tais como SMS e e-mail. O ZabbixServer mantém todo o histórico numa base de dados, *Oracle*, *MySQL* ou *PostgreSQL*, que posteriormente são gerados os gráficos, *slide-shows* e *dashboard* onde é possível uma visualização de toda a informação de forma alternada. Este componente tem, obrigatoriamente de ser instalado para ser possível a monitorização de uma rede, e apenas este, pode ser o único componente instalado para proceder à monitorização, isto é, não é necessário a instalação dos módulos: ZabbixProxy e ZabbixAgent para proceder à monitorização (que serão descritos abaixo)[21], [22].

O servidor onde este componente é instalado não necessita de muitos recursos (memória e CPU).

2.3.4.2- ZabbixProxy

O Componente ZabbixProxy recolhe as informações de uma parte da rede e repassa para o módulo ZabbixServer. Este componente é essencial para uma arquitetura de monitorização distribuída, e muito útil para a recolha assíncrona de dados em redes completamente distintas, onde não seja possível a gestão das regras de roteamento e *firewall* para cada *host* monitorizado. É igualmente útil para trabalhar como ponto de despiste nos casos de instabilidade nas ligações WAN e para diminuir a sobre carga do componente ZabbixServer [22], [23].

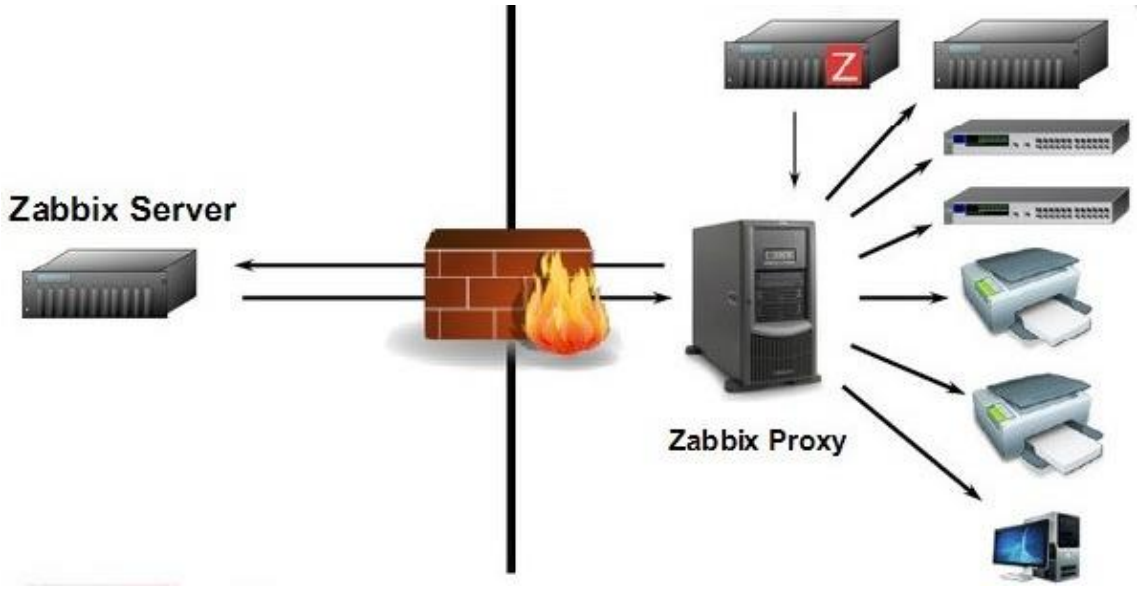


Figura 2.13 – Arquitetura Zabbix Proxy

2.3.4.3- ZabbixAgent

O componente ZabbixAgent é instalado nos *hosts* e permite a recolha de informações mais específicas do sistema operativo, CPU, memórias, e outros. Este possibilita a recolha de informações personalizadas com o uso de *scripts* e, é possível, executar e decidir ações diretamente neste módulo que suporta o IPv6. Há agentes disponíveis em inúmeras plataformas: *Linux*, *Solaris*, *Windows NT*, *Windows Server*, *Sistemas Operativos Windows*, *HP-UX*, *OpenBSD*, *FreeBSD*, *OS X*, e outras. Um agente Zabbix suporta uma função passiva ou ativa.

Numa função passiva o servidor Zabbix (ou Proxy) executa um pedido de um valor ao agente Zabbix. Este processa a informação e retorna o valor ao servidor Zabbix.

A figura abaixo complementa esta informação [24], [25].

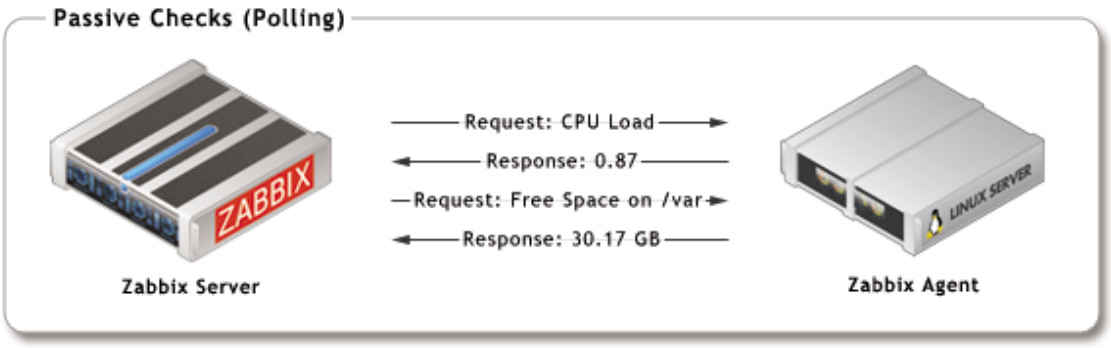


Figura 2.14 – Funcionamento Agente Passivo

Numa função ativa, o agente Zabbix solicita ao servidor Zabbix uma lista de itens ativos, que depois envia ao servidor Zabbix numa periodicidade definida anteriormente, ou caso exista algo inesperado, este envia ao servidor sem que este seja solicitado.

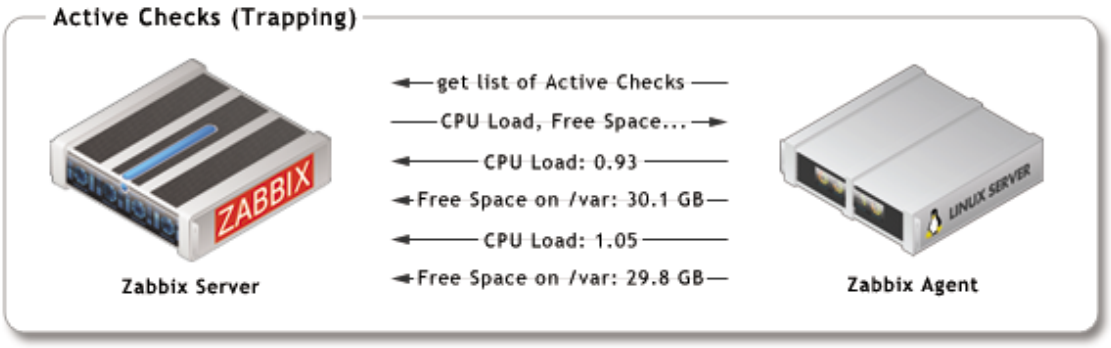


Figura 2.15 – Funcionamento Agente Ativo

Capítulo 3- Contextualização do problema

Neste capítulo, será feita uma análise à Universidade da Madeira para ter uma visão geral da dimensão desta instituição de ensino superior. Para isso serão descritos os três edifícios, a distribuição de alguns serviços internos, o número de postos de trabalho por edifício, número e tipos de utilizadores.

Nos subcapítulos serão descritos e ilustrados vários cenários da rede, com o objetivo de facilitar a contextualização dos problemas, compreender e analisar melhor como é que a rede está dimensionada para ser desenhada uma solução integrada de monitorização e gestão dos recursos de comunicações da Universidade da Madeira.

3.1- Descrição da Universidade da Madeira

A Universidade da Madeira (UMa) é uma instituição de ensino superior público que está dividida em três edifícios situados em diferentes pontos geográficos. Estão localizados na cidade do Funchal na Região Autónoma da Madeira. Os nomes dos edifícios são designados por: edifício da Penteada, edifício da Reitoria e edifício dos Serviços de Ação Social (SASUMA). Os edifícios da UMa estão equipados com cobertura completa Wi-Fi para todos os utilizadores da comunidade académica.

No edifício da Penteada, situado no caminho da Penteada, está localizada a estrutura principal da rede, distribuída por sete andares, sendo três pisos superiores, três pisos inferiores e o piso central. Este é o edifício onde são lecionadas as aulas, com cerca de quinhentos hosts fixos contabilizando as salas de informática. No último triénio, a Universidade da Madeira, acolheu em média, cerca de 3000 alunos por ano. O quadro de docentes é constituído por 208 profissionais distribuídos por cinco Centros de Competências. Segundo o relatório de atividades de 2014 da Universidade da Madeira, “os centros de competência são unidades orgânicas identificadas com áreas disciplinares reconhecidas internacionalmente e orientadas para o desenvolvimento curricular dos investigadores e das respetivas áreas. A Universidade da Madeira integra os centros de competência de Artes e Humanidades; de Ciências Exatas e da Engenharia; de Ciências Sociais; de Ciências da Vida; e de Tecnologias da Saúde”.

No edifício da Reitoria, situado na Rua dos Ferreiros, estão centralizados os serviços da reitoria, os serviços administrativos, serviço de recursos humanos e o Gabinete de Desenvolvimento de Aplicações Informáticas (GDAI). Neste edifício localiza-se alguns servidores importantes, como por exemplo, servidores *web*, a base de dados de alunos e docentes, e algumas plataformas existentes nesta academia. Neste edifício executam as suas tarefas oito funcionários docentes, seis engenheiros, onde todos estes têm no seu posto de trabalho um computador.

O edifício dos Serviços de Ação Social situado na Rua de Santa Maria nº 253 conta com um total de quarenta e sete utilizadores distribuídos pelas categorias: cinco técnicos superiores, nove assistentes técnicos e trinta e três assistentes operacionais. Nesta mesma área de construção está localizado o edifício da residência universitária com a capacidade de cem alojamentos.

Neste documento, o edifício dos Serviços de Ação Social (SASUMA) estará a ser referenciado o conjunto dos dois edifícios (SASUMa e Residência).

3.2- Cenários de rede da Universidade da Madeira

Neste subcapítulo serão descritos e ilustrados vários cenários da rede, com o objetivo de facilitar a contextualização dos problemas a sua compreensão e análise, para melhor perceber como é que a rede está dimensionada para ser desenhada uma solução de monitorização.

Os problemas serão analisados com base nas próximas descrições, mas estes só serão identificados e desenhados no capítulo 4.

3.2.1- Descrição do cenário geral da rede

Este é o cenário mais geral de toda a rede da Universidade da Madeira, onde pode-se verificar na figura abaixo, que qualquer comunicação efetuada para o exterior é filtrada primeiro por uma *firewall* que, por sua vez, está ligada a um *router* para o acesso ao exterior.

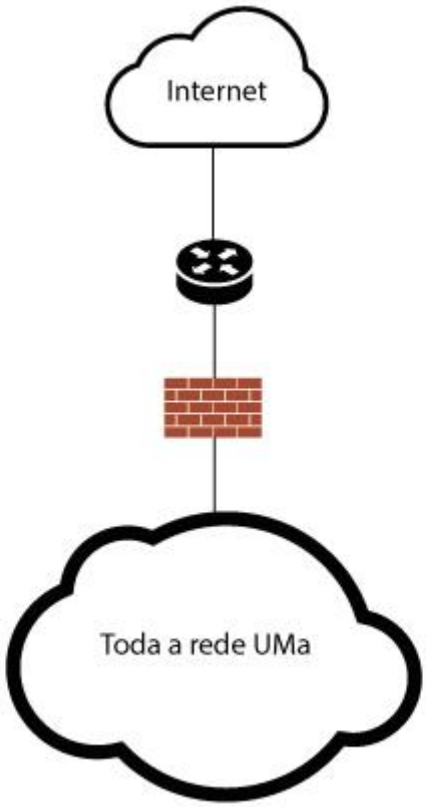


Figura 3.1 – Cenário geral da rede da Universidade da Madeira

3.2.2- Descrição do cenário entre edifícios

O cenário apresentado abaixo na Figura 3.2 representa as ligações entre os edifícios da Universidade da Madeira. A ligação entre o edifício da Penteada e o edifício da Reitoria é realizada através de fibra ótica multimodo subterrâneo a 1Gbps de largura de banda.

Como foi referido no início deste capítulo, o edifício da Reitoria contém serviços essenciais a toda a academia. Devido a esta importância, existia uma redundância nesta ligação. Uma das ligações ficou danificada após o temporal de 20 de Fevereiro de 2010.

A ligação entre a Reitoria e o SASUMa é igualmente em fibra ótica mas apenas com uma largura de banda de 10Mbps.

A ligação entre a SASUMa e o edifício da residência Universitária, por sua vez, é realizada através de um cabo UTP.

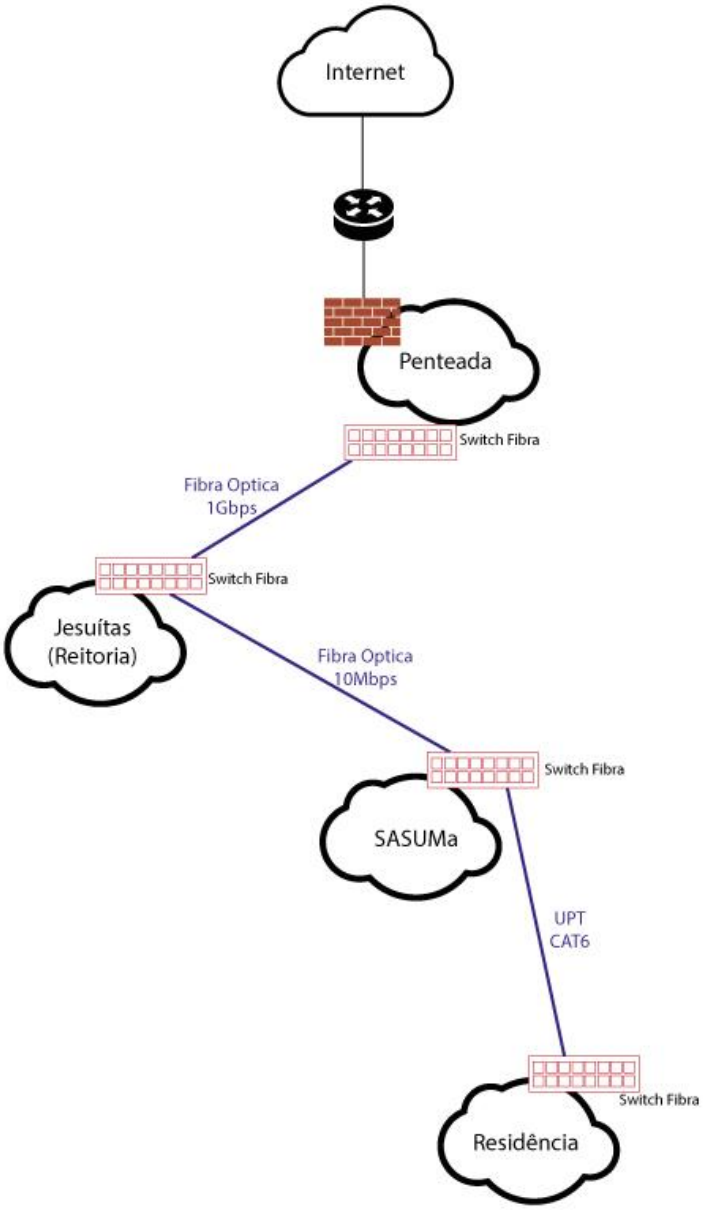


Figura 3.2 – Cenário de rede entre os edifícios da Universidade da Madeira

3.2.3- Descrição do cenário do Backbone do edifício da Penteada

A decomposição hierárquica da rede deste edifício está presente abaixo na Figura 3.3. Como pode-se analisar, é composta por um hierarquia em árvore, com um total de dezasseis bastidores, onde todos estes estão ligados a um bastidor central localizado no piso central. Apenas o bastidor da cantina não está conectado ao bastidor principal. Todo o backbone de edifício é constituído por cabos de fibra ótica multimodo com

uma largura de banda de 1Gbps, apenas o bastidor F tem uma agregação na ligação para 2Gbps. A Tabela 3.1 representa a distribuição dos bastidores por pisos.

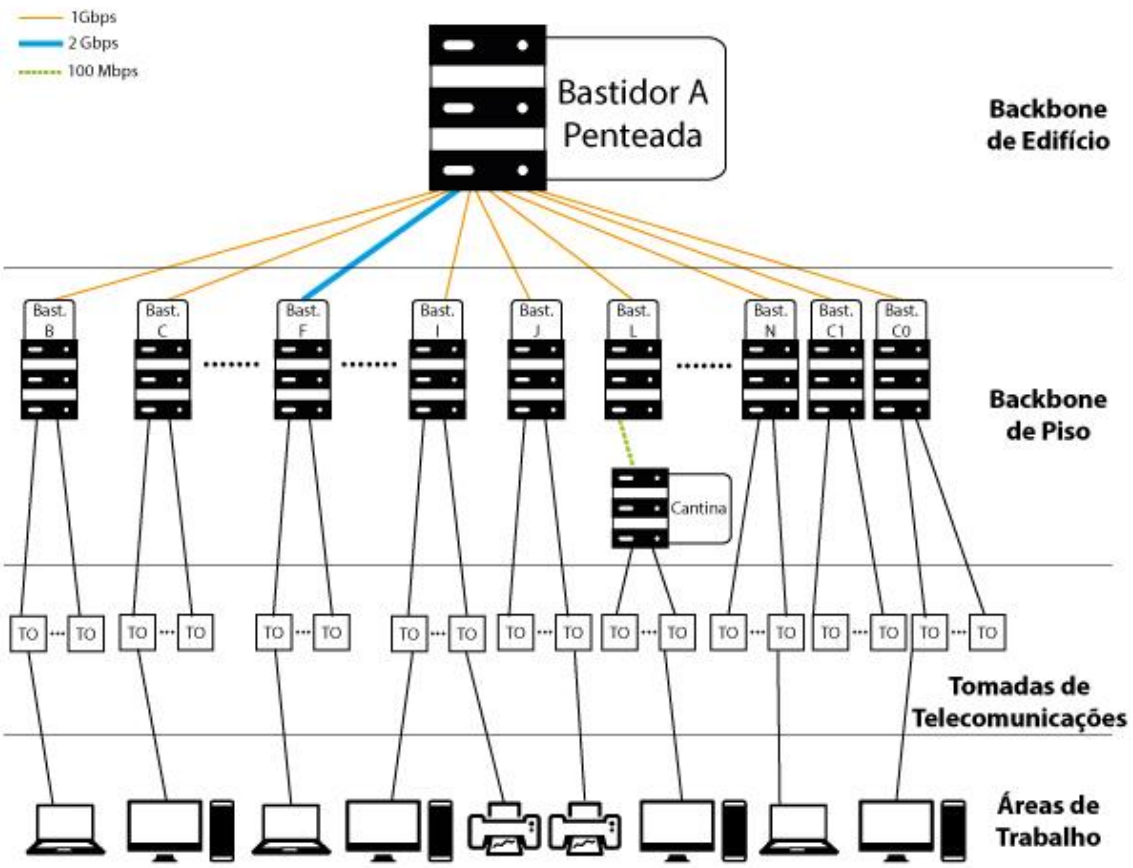


Figura 3.3 – Decomposição hierárquica do backbone do edifício da Penteada

Tabela 3.1 – Distribuição dos bastidores por piso (edifício Penteada)

Piso	Número de bastidores	Nome do Bastidor
3	2	G – H
2	3	E – F – M
1	2	C – D
0	4	A – B – C0 – N
-1	2	I – C1
-2	1	J
-3	2	Cantina – L

3.2.4- Descrição da rede Wi-Fi

Atualmente, a rede Wi-fi é uma das redes mais importantes e utilizadas em todo o mundo, na Universidade da Madeira não é exceção. Esta é uma rede que existe em

todos os edifício desta instituição, o edifício da Penteada contém 114 *Access Points* (APs), o edifício da Reitoria possui 15 APs e o edifício da SASUMA tem 36 APs perfazendo um total de 165 APs. A distribuição dos APs no edifício da Penteada, por pisos, está representada na Tabela 3.2.

Tabela 3.2 – Distribuição dos Access Points por piso (edifício Penteada)

Edifício	Piso	Número de APs
Penteada	3	10
	2	25
	1	22
	0	25
	-1	18
	-2	13
	-3(Cantina)	1

3.2.5- Descrição do cenário das VLANs

Dada a realidade da existência de diferentes tipos e grupos de utilizadores e para diferenciar e/ou restringir os acessos aos serviços, foi criado vários grupos de utilizadores, recorrendo a VLAN. Atualmente, a Universidade da Madeira tem 14 VLAN ativas e 6 inativas perfazendo um total de vinte VLAN configuradas. Como esta instituição é uma universidade, existe dois grupos muito distintos e importantes, dando origem à VLAN1 que é a rede dos docentes e funcionários, e à VLAN2 que é a rede dos alunos. Outra VLAN também com alguma importância é a VLAN6, esta é a VLAN de toda a infraestrutura Wi-fi, descrita no ponto anterior. Estas são as três VLANs mais usadas e importantes.

Como é possível verificar na Figura 3.4 existe VLAN que estão conectadas diretamente à *firewall* para a gestão das mesmas e outras ligadas apenas aos switch para os acessos internos.

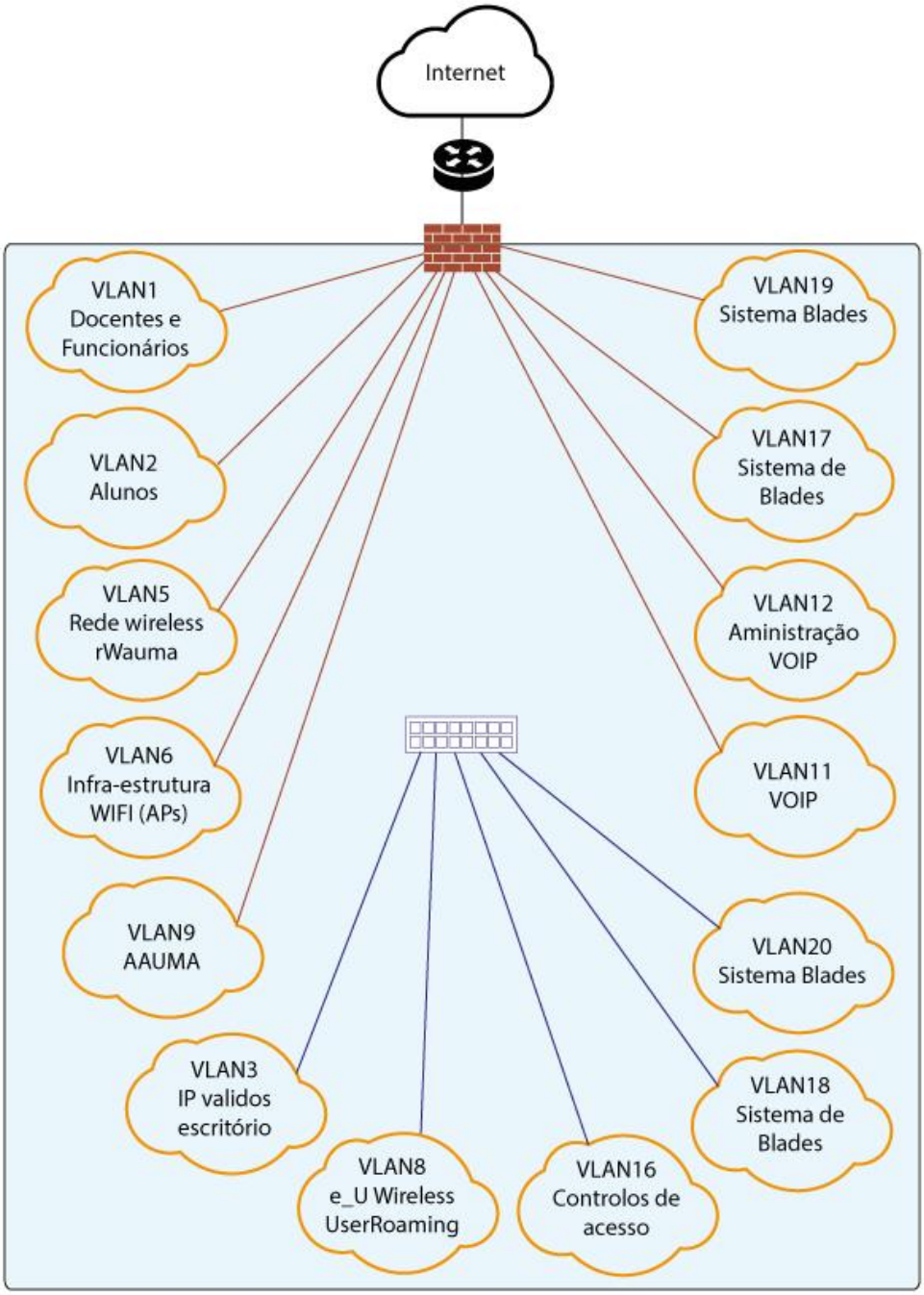


Figura 3.4 – Cenário da VLANs existentes na Universidade da Madeira

Tabela 3.3 – VLANs existentes na Universidade da Madeira

VLAN	Designação da Rede	Destinatários
VLAN1	Docentes e Funcionários	Docentes e Funcionários da UMa e dos SASUMa
VLAN2	Alunos	Alunos da UMa
VLAN3	IPs válidos	Router, Servidor DNS externo, etc.
VLAN5	Rede wireless rwauma	Laboratórios Salas de aula de informática, WPA Pre-shared Key
VLAN6	Infra-estrutura Wi-Fi	APs Wireless
VLAN8	e-U Wireless	Utilizadores em roaming na rede e-U
VLAN9	AAUMa	AAUMa
VLAN11	VoIP	Docentes e Funcionários da UMa
VLAN12	Administração VoIP	Gestão de equipamentos VoIP
VLAN16	Controlo acessos interno SALTO e externo NET2	Controlo de acessos internos e externos UMa Posto R (Recepção) Parque Jesuítas
VLAN17	Sistema de Blades Rede Gestão	Gestão dos Servidores Blade, Fabric Interconnect e Storage NetApp
VLAN18	Sistema de Blades	VLAN *iSCSI/*vMotion
VLAN19	Sistema de Blades	VLAN *vMotion*/iSCSI
VLAN20	Sistema de Blades	VLAN Hosts de VMware

3.2.6- Descrição ao bastidor central do edifício da Penteada

O bastidor central do edifício da Penteada é o mais importante de todos os bastidores da Universidade. Este bastidor é composto por onze *switches*, distribuídos da seguinte forma:

- Dois *switches* são designados por *switches* "Core", estão ligados entre si, existem as ligações em fibra ótica entre os bastidores deste edifício, e contém a ligação com o edifício da Reitoria;
- Dois *switches* ligam a várias VLAN, e têm uma particularidade, está implementado um módulo de 10Gbps entre eles, pois um dos switches está ligado a servidores importantes;

- Um *switch*, este apenas serve de apoio à VLAN2;
- Seis *switches* ligados em Stack, estes funcionam como se fosse apenas um.

3.3- Metodologia para testar e selecionar a ferramenta de Gestão

Esta metodologia foi fundamentada no artigo "Comparative analysis of monitoring system for data Networks" que está na bibliografia identificada com o número 24. Para a seleção da ferramenta de monitorização será considerado os seguintes critérios:

- Preço – para a decisão sobre qual o sistema de monitorização que irá ser utilizado, o preço é sempre um dos critérios fundamentais. Infelizmente, diversas vezes, o preço é superestimado e muitas empresas não analisam bem este parâmetro, pois este deve ser analisado proporcionalmente aos custos de trabalho que irá ser reduzido ao agilizar os processos.
- Requisitos do sistema – este critério avalia os requisitos mínimos para iniciar o sistema, tanto em termos de carga como também as aplicações de suporte.
- Interface do utilizador – Critério muito difícil de ser analisado, pois este depende muito das perspetivas do utilizador, é praticamente impossível obter uma avaliação objetiva. Neste projeto será feita uma análise pessoal a partir do meu ponto de vista, ao nível da visualização da rede, exibição de gráficos e outros pontos que venham a ser revelantes para a análise a este critério.
- Dificuldade na implementação – Critério que avalia a dificuldade de instalação e configuração básica para iniciar o sistema de monitorização. A avaliação está direcionada especialmente para o tempo de implementação, a qualidade da documentação que descreve todo o processo e o tempo e/ou dificuldade na inserção de *hosts* para serem monitorizados.
- Velocidade de resposta à falha – Este critério avalia a velocidade de resposta com base no tempo, do sistema à falha de qualquer elemento da rede.
- Procura automática – Avalia se a ferramenta verifica automaticamente uma área a monitorizar ou procura nós na rede para a monitorização. Este tipo de função utiliza os protocolos SNMP e ICMP. Neste critério o que será avaliado é

essencialmente a qualidade de pesquisa, a velocidade e o reconhecimento da topologia real da rede.

- Métodos de notificação – Avaliação da perspetiva da informação da situação da rede a enviar ao administrador. Os sistemas típicos são o SMS e o e-mail.
- Funções adicionais – Avalia funções adicionais, fora do padrão dos sistemas de monitorização.[26]

Capítulo 4- Análise e Desenho da solução

Neste capítulo será desenhada uma solução para cada cenário criado no subcapítulo 3.2- Cenários de rede da Universidade da Madeira, tendo em conta sempre no mínimo três características do modelo FCAPS, a gestão da performance, gestão de falhas e gestão de *accounting*, pois sem este seria difícil chegar a dados de performance.

De seguida, são apresentados alguns conceitos importantes que dizem respeito ao estado dos dispositivos e níveis de gravidade das ligações a monitorizar.

Quando é referido que uma ligação está "*down*" ou "*up*", refere-se ao estado operacional (*Operational Status*). No caso de a ligação estiver "*down*, quer dizer que não existe qualquer tráfego na ligação, caso contrário significa que estaria a "*up*".

Quando é mencionado que uma porta está "*down*" ou "*up*", refere-se ao estado físico (*Operacional Status*) da porta do *hardware*, quando esta apresentar o estado de "*down*", significa que está desligada ou não existe qualquer ligação conectada na porta específica, caso contrário apresentará "*up*".

Tendo em conta os problemas levantados anteriormente e que serão identificados nos próximos subcapítulos, foram definidos níveis diferentes de gravidade e importância que se considera mais ajustados para os problemas neste projeto. Através de uma pesquisa rápida na web, estes níveis fazem parte de boas práticas e são os mais usados pelas ferramentas de gestão. Os níveis de gravidade definidos para este projeto serão:

- Informação - apenas informa de algo que não prejudica a rede, mas é importante informar.
- Aviso - algo que está a acontecer, que está a afetar uma pequena parte da rede, e poderá não precisar de uma intervenção.
- Média - algo que está a acontecer, que está a afetar uma pequena parte da rede. Se não tiver intervenção, não é grave, mas fica o alerta feito, pois se este persistir, uma intervenção terá de ser feita.
- Alta - algo que está a acontecer, que está a afetar uma parte importante da rede. Esta precisa de uma intervenção rápida por parte do gestor.
- Desastre - algo aconteceu, que está a prejudicar gravemente a rede e necessita de uma intervenção urgente.

A Universidade da Madeira não dispõe atualmente de condições financeiras para a implementação de uma plataforma paga. Seguindo o princípio do open source descrito na introdução, será apresentado uma ferramenta totalmente gratuita, que suporte as centenas de equipamentos ativos existentes na Universidade da Madeira, que seja de fácil implementação e configuração. Permitindo igualmente a utilizadores com conhecimentos avançados, adicionarem funcionalidades de acordo com as necessidades do dia-a-dia. Uma ferramenta que apresente ao gestor de rede os alertas através de email e/ou SMS personalizados permitindo especificar quem recebe um certo tipo de alerta, mostrar estatísticas e performance da rede com vários tipos de gráficos em tempo real, geração de relatórios e histórico de problemas.

4.1- Análise e Desenho da solução do cenário geral da rede

Com base na descrição do subcapítulo 3.2.1- , tendo como referência a Figura 3.1 denota-se que um ponto importante a ser monitorizado é a ligação entre a firewall e o router pois se esta for desativada ou existir falhas a Universidade da Madeira poderá ficar apenas com a rede interna a funcionar, e todos os pedidos ao exterior serão impossibilitados.

A monitorização a esta ligação deverá consistir numa análise ao tráfego e ao *Status* dos dois *hardwares*. Se o tráfego atingir valores exagerados, fora do padrão normal de funcionamento, durante um determinado espaço temporal, deverá ser emitido um alerta, pois esta poderá estar a ser alvo de um ataque fazendo obstruir a comunicação. Relativamente ao *status*, este será igualmente importante pois se estiver “down” isso poderá corresponder a um problema físico, tendo de ser rapidamente emitido um alerta.

4.2- Análise e Desenho da solução entre edifícios

Com base na descrição do subcapítulo 3.2.2- , tendo como referência a Figura 3.2, temos a perceção que o edifício da Reitoria é um edifício importante e a sua ligação com o edifício da Penteada é extremamente crítica. Se esta falhar, não é apenas o

edifício da Reitoria que fica isolado mas sim ficariam igualmente sem ligações ao exterior e ao edifício da Penteada, o edifício da SASUMa.

Para uma monitorização correta a esta ligação será efetuada uma análise ao tráfego tendo em conta os padrões diários nesta ligação, alertando caso sejam excedidos ou ficar sem tráfego em momentos em que a academia está no ativo ou as portas dos *switches* onde estas ligações estão conectadas ficarem desativadas sem nenhum motivo aparente, pois isto, poderá indicar que a ligação estará a ser atacada ou que o *hardware* está com falhas.

4.3- Análise e Desenho da solução do backbone do edifício da Penteada

Com base na descrição do subcapítulo 3.2.3- , tendo como referência a Figura 3.3, denota-se que as ligações entre bastidores são de alguma importância, pois nestes bastidores estão conectados os Centros de Competências e os seus utilizadores (alunos e docentes). Atualmente não existe conhecimento sobre o tráfego existente diariamente nestas ligações.

Tendo em conta a importância acima referida dos bastidores distribuídos pelos pisos, será efetuada uma monitorização ao tráfego. Para verificar a performance, será analisado os valores padrão do tráfego diário. Se este for alterado para níveis muito elevados ou nenhum, será efetuada uma monitorização ao estado operacional da porta, verificando se esta encontra-se “down” ou “up”. Nestes dois caso será emitido um alerta para uma rápida solução do problema.

4.4- Análise e Desenho da solução da rede wi-fi

Com base na descrição do subcapítulo 3.2.4- , apresenta-se uma pequena análise para verificar o quanto esta rede é importante. Tendo como exemplo: ”No edifício da Penteada tem cerca de 3000 alunos e 208 docentes. Atualmente existe uma percentagem muito elevada de pessoas que possuem um ou mais dispositivos com acesso ao wireless. Supondo que cada pessoa tem pelo menos um dispositivo com acesso ao wireless, teríamos diariamente cerca de 3208 utilizadores conectados aos

100 APs". Este exemplo permite supor que poderia estar cerca de 30 utilizadores por cada APs ou em caso de falha nesta rede estaria cerca de 3000 utilizadores sem acesso à internet, e a plataformas existentes na Universidade. Os APs são compostos apenas por uma porta *ethernet* e um emissor Radio.

A monitorização aos APs será dividida em várias regras, isto é, será emitido vários tipos de alarmes diferentes e vários níveis de gravidades:

- Quando a porta ethernet do AP estiver "down", o nível de gravidade deverá ser "Média";
- Quando o emissor Radio não estiver a enviar frequências ou estiver "down", o nível de gravidade deverá ser "Média";
- Se existir tráfego na porta ethernet e não existir qualquer emissão de frequência Radio, o nível de gravidade deverá ser "Média";
- Definir número mínimo de utilizadores em cada AP, quando esse número for ultrapassado, será emitido um alerta, o nível de gravidade deverá ser "Informação";
- Se o tráfego da ligação ethernet atingir o limite permitido pelo hardware (AP), isto significará que o hardware está com sobrecarga, o nível de gravidade deverá ser "Aviso".

4.5- Análise e Desenho da solução á arquitetura lógica das VLANs

Com base na descrição do subcapítulo 3.2.5- , tendo como referencia a Figura 3.4, irá ser feita uma análise a todas as VLANs, irá ser dividido em dois grupos de análise. O grupo das VLANs críticas e não críticas, as VLANs não críticas não significa que serão colocadas de parte, mas sim irão ter outros critérios de análise, que serão abordados posteriormente.

No grupo das VLAN críticas será uma solução com base no tráfego e no estado operacional em todas as ligações entre bastidores do edifício da penteada e nas ligações entre edifícios. Em relação ao tráfego emitirá um alerta, quando este atingir valores superiores do que 90% da largura de banda nas ligações. Se estes valores tornarem-se padrões no horário normal de funcionamento da Universidade indicará que será necessário evoluir as ligações ou até mesmo o *hardware*. As VLAN não críticas

irá igualmente ser feita uma análise ao tráfego e ao estado operacional da ligações mas apenas no edifício da Penteada.

4.6- Análise e Desenho da solução ao bastidor central do edifício da Penteada

Com base na descrição do subcapítulo 3.2.6- , a monitorização e os alertas serão divididos com os níveis de gravidades da seguinte forma:

- Em todos os Switches:
  - Quando um Status de uma porta for alterado, a gravidade deverá ser "informação".
- Nos Switches "Core":
  - Quando alguma das ligações entre os bastidores do edifício da Penteada atingir valores muito acima dos padrões, que serão definidos posteriormente, o nível de gravidade deverá ser "Média";
  - Quando alguma das portas de ligação aos bastidores do edifício da Penteada estiver "down", o nível de gravidade deverá ser "Alta";
  - Quando a ligação com o edifício da Reitoria atingir níveis muito acima dos padrões, que serão definidos posteriormente, o nível de gravidade deverá ser "Alta";
  - Quando a porta de ligação ao edifício da Reitoria estiver "down", o nível de gravidade deverá ser "Desastre";
  - Quando a ligação entre switches "Core" atingir níveis acima dos padrões, que serão definidos posteriormente, o nível de gravidade deverá ser "Alta";
  - Quando a porta de ligação entre switches "Core" estiver "down", o nível de gravidade deverá ser "Desastre".
- Nos restantes Switches:
  - Quando alguma das ligações das VLANs com a Firewall atingir níveis acima dos padrões, que serão definidos posteriormente, o nível de gravidade deverá ser "Alta";

- Quando alguma porta das ligações das VLANs com a Firewall estiverem "down", o nível de gravidade deverá ser "Desastre";
- Quando as ligações dos módulos de 10Gbps atingirem níveis acima dos padrões, que serão definidos posteriormente, o nível de gravidade deverá ser "Alta";
- Quando alguma porta dos módulos de 10Gbps estiver "down", o nível de gravidade deverá ser "Alta".

4.7- Seleção da ferramenta

4.7.1- Comparação das ferramentas

O sistema de monitorização foi selecionado com base na metodologia descrita no subcapítulo 3.3- , em documentação existente do próprio *software*, com o apoio de artigos que abordam este tema, e através de uma instalação realizada em ambiente virtual que será descrita de seguida.

Para o cenário de testes foi utilizado um ambiente virtual sobre a plataforma Hyper-V. Foi criado um servidor com o sistema operativo Debian com requisitos mínimos para cada ferramenta, podendo assim, avaliar também, o grau de dificuldade na instalação e configuração. Foi ligado um *Switch* e um computador ao servidor para ser executado alguns testes para a avaliação.

- Preço – Do ponto de vista do preço as ferramentas Icinga e Zabbix apenas têm versão gratuita. O Zenoss e o Nagios, têm uma versão paga e uma versão gratuita. Todas as ferramentas foram testadas com a versão gratuita.
- Requisitos do sistema – Este campo foi baseado na documentação das ferramentas. Em primeiro lugar, vem o Zabbix com um CPU PII 350MHz e 256Mb de RAM. [27]. Em segundo lugar, o Nagios com um CPU 1GHz e 512Mb de RAM[28]. Em terceiro lugar, o Icinga um CPU 2GHz e 4GB de RAM.[29]. Em último, o Zenoss com CPU Dual Core com 4GB de RAM.[30]

  Estes valores foram estimados para uma rede com 100 equipamentos a serem monitorizados, visto que acima deste valor, todos os requisitos de todas as ferramentas eram proporcionais, isto é, mesmo que seja para monitorizar 1000 equipamentos a classificação das ferramentas continua a mesma.

- Interface do utilizador – É muito difícil avaliar objetivamente a interface com o utilizador, pois, esta avaliação será subjetiva. Todos eles têm uma interface *web*. Do meu ponto de vista, o Zabbix é o mais "UserFriendly", devido a ser muito parecido com a maioria dos *websites* existentes atualmente na internet e fácil acesso ao que necessitamos. Segue-se o Zenoss com uma interface igualmente muito boa. O Icinga é um pouco diferente, é mais confuso para gerir os hosts e os grupos. Por último, no Nagios, a avaliação é mais subjetiva devido ter vários *plugins* de *interfaces*, isto é, o utilizador pode escolher uma de várias interfaces, o que pode torná-lo para outros utilizadores a ferramenta com a melhor interface
- Dificuldade na implementação – Os mais simples de implementar foi o Zabbix, existe muita documentação oficial sobre os passos para efetuar a instalação e em diversas línguas. Um utilizador comum sem conhecimentos nesta área consegue instalar esta ferramenta. No Nagios é necessário instalar plugins para poder estar pronto a monitorizar, como consequência levou um pouco mais de tempo na instalação devido à pesquisa dos melhores plugins para a monitorização. Tendo gerado alguns erros com alguns plugins, mas foram corrigidos com a ajuda de websites não oficiais. O Zenoss e o Icinga tiveram alguns problemas de compatibilidade, o que gerou alguns erros, e algum tempo para corrigir. Com isto, não significa que o Zenoss e o Icinga sejam difíceis de implementar, pois foi com a ajuda da documentação existente na web que consegui resolver os problemas pontuais.
- Velocidade de resposta à falha – A ideia original deste parâmetro foi a avaliação do tempo de resposta com base no tempo. No entanto, durante o teste verificou-se que este não seria suficientemente objetivo porque as ferramentas testadas permitiram definir o intervalo de verificação da rede. Após esta verificação decidiu-se considerar a ferramenta que possibilita o menor número de intervalo. O Zabbix e o Zenoss possibilitam a verificação mínima de um segundo enquanto o Nagios e o Icinga o mínimo é de um minuto.

- Procura automática – Todas a ferramentas executam a pesquisa automática na rede de forma simples. O Zabbix é o único que não cria automaticamente um desenho da rede. O desenho tem de ser criado manualmente.
- Métodos de notificação - Todas as ferramentas têm vários tipos de notificação, todas elas alertam por SMS, correio eletrónico e contêm vários tipos de gráficos.
- Funções adicionais – Todas as ferramentas permitem adicionar funções, todas elas permitem a um utilizador com experiência na área, desenvolver plugins e addons para as ferramentas. A pontuação mais alta vai para o Nagios e o Icinga porque através de uma pesquisa rápida percebemos que existe imensa informação, plugins e addons oficiais e não oficiais para estas duas ferramentas, enquanto no Zabbix e Zenoss a maior parte dos plugins e addons provêm de *websites* oficiais.

4.7.2- Resultado da comparação

Para a demonstração dos resultados obtidos nas comparações e para melhor compreensão, foi utilizada a tabela 4.1 para representar a classificação através de pontuação. Usou-se a numeração de 1 a 4, sendo o 4 o valor mais elevado.

Tabela 4.1 – Pontuação das ferramentas de gestão e monitorização

Critérios	Icinga	Nagios Core	Zabbix	Zenoss
Preço	4	4	4	4
Requisitos do sistema	2	3	4	1
Interface do utilizador	3	3	4	4
Dificuldade na implementação	2	3	4	2
Velocidade de resposta à falha	3	3	4	4
Procura automática	4	4	3	4
Métodos de notificação	4	4	4	4
Funções adicionais	4	4	3	3
Total	26	28	30	26

É de salientar que nenhuma das aplicações poderá ser considerada como não prestável. Todas cumpriam os objetivos deste projeto. A perda por parte dos sistemas Icinga e Zenoss poderá ser provavelmente a sua filosofia de abordagem à gestão de rede.

O triunfo vai para a ferramenta Zabbix, com dois pontos de diferença para o segundo classificado o Nagios. Como o Nagios tem uma versão paga, e o Zabbix não contem nenhuma versão paga, foi efetuado um teste no mesmo cenário com a mesma metodologia à ferramenta Nagios XI para compararmos o Zabbix a uma ferramenta paga. Foi utilizada a versão de sessenta dias completa sem nenhuma restrição. Surpreendentemente o Zabbix continua a ganhar. O que mudou no Nagios XI foi o facto de ser muito simples a sua implementação, e após a instalação está tudo pronto para monitorizar a rede, sem a necessidade da instalação de plugins. Contudo, o Nagios XI é necessário pagar milhares de euros enquanto o Zabbix é gratuito, e após a instalação está igualmente pronto a monitorizar a rede.

Por curiosidade, foi consultado uma ferramenta fornecida pela Google designada por o "Google Trends" onde apresenta gráficos com a frequência que um termo é procurado em várias regiões do mundo. Foi avaliada a frequência com que é pesquisada as quatro ferramentas obtendo o gráfico da Figura 4.1. Podendo analisar que o Nagios, em 2004 era a ferramenta mais procurada com uma diferença imensa em relação às outras. Ao longo dos anos, nota-se um decréscimo na frequência de pesquisas do Nagios e um aumento em relação às outras ferramentas. Atualmente, a ferramenta Zabbix está a se tornar popular com uma diferença mínima em relação ao Nagios.

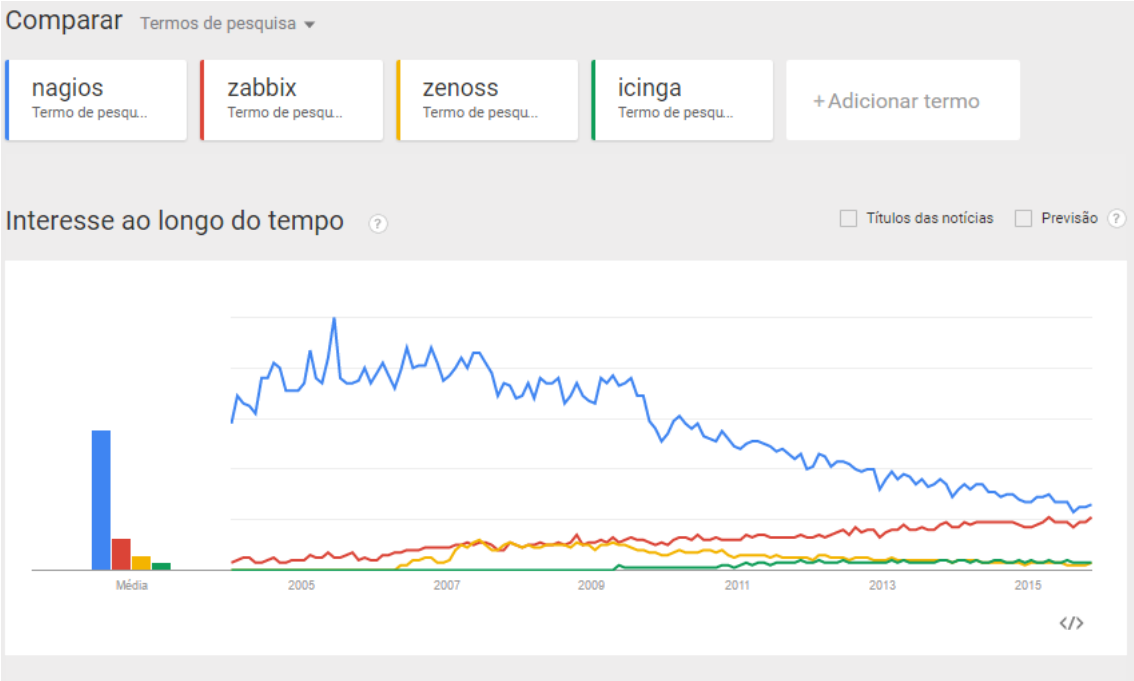


Figura 4.1 – Grafico fornecido pelo Google Trends

Capítulo 5- Implementação da solução

Dada a dimensão da Universidade da Madeira, foi necessário restringir a implementação da solução à rede *wireless*, aos equipamentos: Router e Firewall, e às ligações mais importantes, tais como, as ligações backbone e a ligação entre o edifício do Jesuítas e Penteada.

5.1- Instalação da ferramenta Zabbix

Numa primeira fase foi instalado a ferramenta Zabbix num computador disponibilizado pelo gabinete de informática para ser efetuado os primeiros testes à ferramenta num cenário real. O computador tinha as seguintes características: o sistema operativo Linux Debian 7 (Wheezy) de 32bits, um CPU Pentium 4 com 1GB de RAM e 40 GB de disco. Foi instalado na VLAN onde está localizado outros servidores. Foi configurado um acesso ao exterior por SSH, para este estar sempre acessível.

Em anexo encontram-se os procedimentos que foram seguidos para a instalação desta ferramenta.

5.2- Arquitetura da solução

Através do levantamento das necessidades e dos problemas relativamente a todo o sistema informático da Universidade da Madeira, foi possível identificar as principais falhas nas áreas funcionais do modelo FCAPS descrito no capítulo 2 - Contexto Tecnológico, particularmente na gestão de Falhas, Desempenho e Accounting.

A ferramenta Zabbix tem como principal tarefa, a gestão e monitorização de toda a rede da Universidade da Madeira, atuando particularmente nos modelos do FCAPS acima referidos. Na implementação do Zabbix, a solução desenhada, como se pode observar na Figura 5.1, baseia-se numa arquitetura distribuída, utilizando uma topologia funcional tipo gestor-agente, mas principalmente pelo SNMP, descrito no capítulo 2 Contexto Tecnológico.

Foram criadas regras com o objetivo de criar nomenclaturas para cada tipo dispositivo de rede, uma forma de organização para ser mais fácil a visualização na ferramenta, e no futuro facilitar a incorporação de novos equipamentos ao Zabbix.

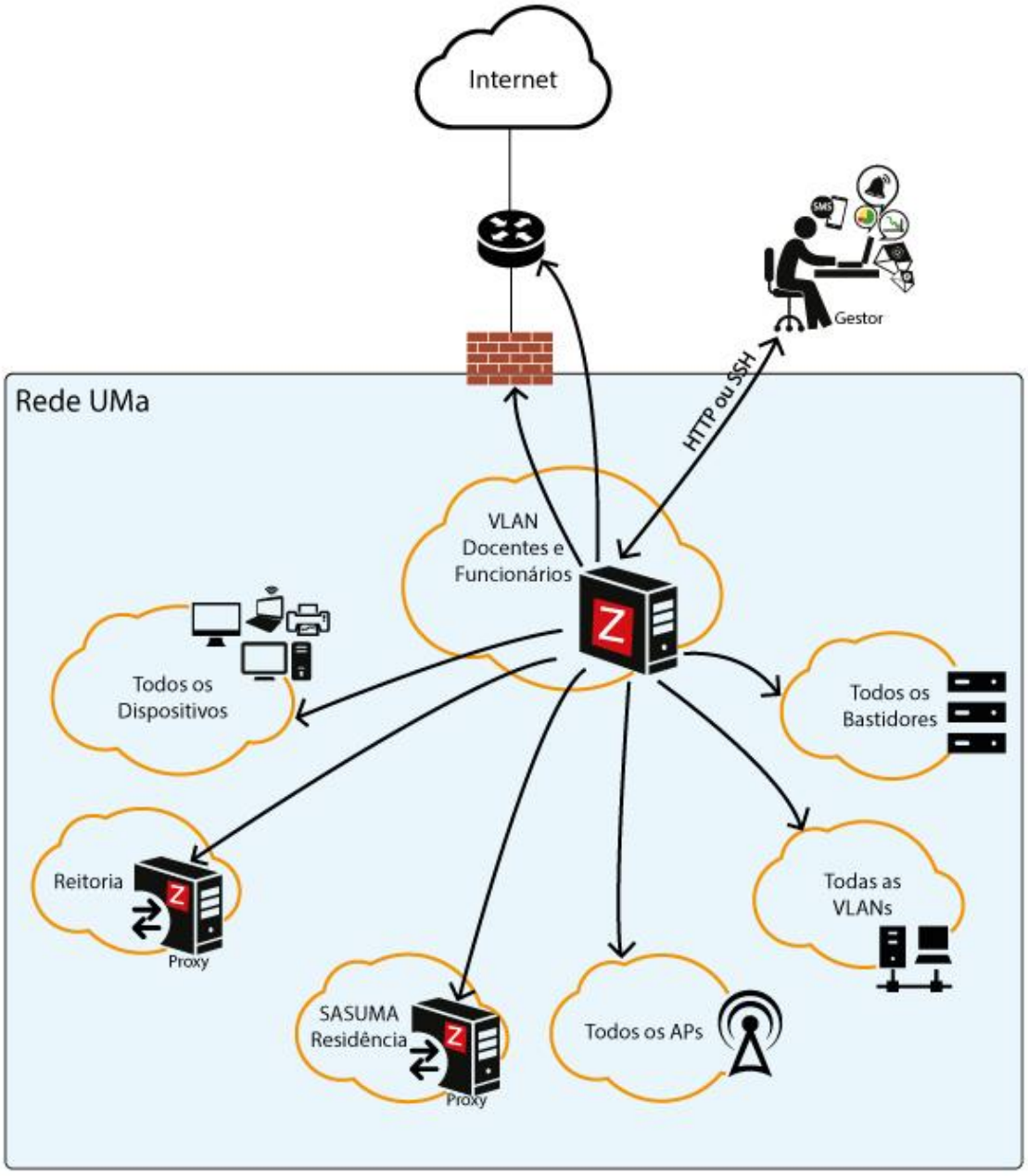


Figura 5.1 – Arquitetura da solução

Nesta arquitetura, a entidade gestor do Zabbix (Zabbix Server) situado no edifício da Penteada, encontra-se a funcionar na VLAN dos docentes e funcionários, tendo permissão para atuar sobre qualquer um dos sistemas de toda a rede da Universidade da Madeira. Para uma melhor gestão e desempenho da ferramenta e vista a dimensão da rede, uma solução seria a criação de dois proxys do Zabbix. Um na rede da reitoria para monitorizar todos os equipamentos e serviços instalados nesse edifício e outro na

rede da SASUMA que monitorizava a rede da residência. Assim, apenas o dashboard dos proxys eram consultados no Zabbix Server evitando uma sobrecarga do mesmo.

É importante salientar que a ferramenta consegue analisar qualquer equipamento, mesmo sem a instalação do seu agente, desde que o mesmo contenha suporte ao protocolo SNMP. O "*SNMP COMMUNITY*" teve de ser alterado em alguns equipamentos durante a fase de implementação. Estas situações serão descritas neste capítulo posteriormente.

Na prática, a monitorização destes sistemas irá consistir numa observação periódica, no qual o gestor de rede conseguirá obter mais conhecimento sobre o estado atual da rede podendo atuar agilmente e de modo mais eficiente sobre a mesma. Esta gestão será direcionada para o controlo e monitorização na utilização dos recursos de comunicação da rede informática.

Nos subcapítulos seguintes segue-se a apresentação dos métodos e processos da implementação da arquitetura no sistema de monitorização Zabbix na rede informática da Universidade da Madeira.

5.2.1- Criação de templates

Um template é um conjunto de entidades que podem ser convenientemente aplicados a vários *hosts*. Essas entidades podem ser *itens*, *triggers*, gráficos, aplicações e outros. [31] Como muitos equipamentos são idênticos ou semelhantes, existe um conjunto de entidades que ao serem criadas para um *host*, podem ser utilizadas para muitos outros. Estas podiam ser copiadas para cada *host* criado, mas seria um trabalho manual muito extenso no caso de criar centenas de *hosts*. Sendo assim, após criar um template e associá-lo a vários *hosts*, caso seja necessário modificar, eliminar ou adicionar a um conjunto de equipamentos pertencentes a um determinado template, não é necessário executá-lo um a um, bastando apenas executar a ação no template que este aplicará em todos os *hosts* associados a esse template. Um exemplo prático na Universidade da Madeira são os Access Points, existe 150. Imaginemos que quando fosse para adicionar ou retirar algum *trigger*, teria de ser feito nos 150 manualmente

um a um, isto seria um trabalho exaustivo. Assim, criado um template geral para os Access Points, reduz a carga de trabalho e simplifica a configuração no Zabbix.

Numa primeira fase, com base nos equipamentos existentes na Universidade, foi analisado os templates disponibilizados por defeito pela ferramenta. Verificou-se que apenas existia um template para o protocolo SNMPv2 e que alguns dos equipamentos não suportam esse protocolo mais sim SNMPv1, o que levou à criação de novos templates para esta versão do protocolo. O Zabbix permite a criação dos próprios templates com os *itens* específicos para cada tipo de equipamento. Neste caso foi criado um template para a descoberta de *itens* nos equipamentos com protocolo SNMPv1.

Para uma boa gestão dos equipamentos de rede foram criados três templates.

Os templates são os seguintes:

- APs_UMa – Este template está adaptado ao modelo dos APs de toda a Universidade. Os APs têm todos o mesmo modelo. Este template está associado a outro template existente no Zabbix, cujo nome é "Template SNMP Device" onde permite a verificação e descoberta dos *itens* a serem geridos existentes nos APs.
- Switches_UMa_SNMPv1 – Este template contém dois templates associados. Este está adaptado aos Switches com o template "Template SNMPv1 Device" cujo a versão do protocolo SNMP é a versão 1. O outro é o "Template ICMP Ping" onde está configurado triggers específicos para o protocolo ICMP.
- Switches_UMa_SNMPv2 – Este é idêntico ao template acima descrito, apenas é diferente na versão do protocolo SNMP.

5.2.2- Criação de grupos

O Zabbix organiza os equipamentos por grupos, deste modo serão criadas regras para a criação dos mesmos. O grupo irá conter todos os dispositivos geridos de um certo tipo de equipamento. Este terá o nome do tipo de dispositivo gerido e o nome do edifício onde está instalado. Estes serão descritos adiante e a Figura 5.2 representa a estrutura dos mesmos no edifício da Penteada. As nomenclaturas também serão descritas nos subcapítulos seguintes.

A regra na criação do nome do grupo:

- "tipo de dispositivo"_"nome do edifício onde está instalado".

  Exemplo: Os switches que estão localizados no edifício da penteada irão pertencer ao grupo "Switches_Penteada".

A Universidade da Madeira, atualmente, contém somente um Router e uma Firewall. Serão criados um grupo para cada equipamento, com o objetivo no futuro, ao serem adicionados novos equipamentos, o grupo já existente.

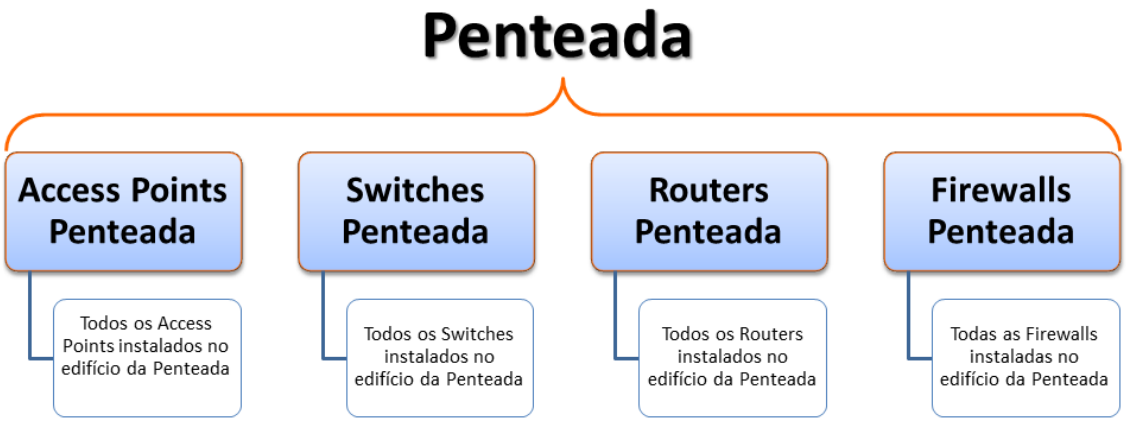


Figura 5.2 – Estrutura para a criação dos grupos

Futuramente poderão ser criados mais grupos, como por exemplo, "Servidores Penteada", "Serviços Penteada", "Computadores Penteada", e outros.

5.2.3- Criação dos equipamentos geridos

Seguindo a lógica da criação dos grupos, igualmente será criado regras e nomenclaturas para a criação dos nomes dos equipamentos geridos e a introdução dos mesmos na ferramenta. Os templates disponibilizados pela ferramenta foram modificados e adaptados para alguns dos equipamentos. As regras serão descritas nos próximos subcapítulos.

5.2.3.1- Criação dos Access Points

Os Access Points são os equipamentos com maior número de dispositivos na rede. Pretende-se a criação de uma regra na atribuição do nome, quando estivermos a trabalhar com a ferramenta, consigamos identificar e localizar o aparelho, através do nome.

A regra para a criação do nome:

- AP_”piso onde está localizado”_”últimos dois octetos do IP” Exemplo: um Access Point que esteja localizado no piso -2 com um IP 192.168.1.1 terá o nome “AP_P-2_1.1”

5.2.3.2- Criação dos Switches

Os Switches terão uma configuração diferente, pois estes estão localizados dentro de bastidores.

A regra para a criação do nome:

- Bast_”Letra do bastidor onde está instalado o equipamento”_”modelo do equipamento”_”número do último octedo do IP do equipamento” Exemplo: Um Switch com um modelo Cisco 3200, localizado no bastidor A com o IP 192.168.1.20 terá o nome “Bast_A_Cisco3200_20”

5.2.3.3- Criação do Router e Firewall

Visto que em toda a infraestrutura de rede apenas existe uma firewall e um router, o nome será composto apenas pelo tipo de dispositivo e as primeiras quatro letras do nome do edifício onde está localizado.

A regra para a criação do nome:

- “Tipo de dispositivo”_”edifício onde está localizado” Exemplo: o Router localizado no edifício da Penteada terá o nome “Router_Pent”

5.3- Criação de triggers

Para a criação dos triggers no Zabbix existe alguns parâmetros que é necessário ter em conta. Existe triggers que serão criados nos templates devido à igualdade de funções dos equipamentos, como por exemplo nos access points. Outros terão de ser criados individualmente em cada dispositivo devido a particularidades nas suas funções.

O Zabbix permite obter uma representação mais “humana” dos valores recebidos podendo usar value mapping (mapas de valor) que contêm o mapeamento dos valores numéricos e representações de sequências. Estes mapeamentos podem ser utilizados nos triggres, no frontend e nas notificações enviadas por email ou SMS.

Por exemplo, um item que tem o valor 0 ou 1 pode ser usado um mapeamento de valor para representar os valores em formato legível:

- ‘0’ =>”não disponível”
- ‘1’=>”disponível”

O Zabbix disponibiliza vários *value mapping*, neste projeto irão ser utilizados dois desses mapeamentos em todos os dispositivos.

A Figura 5.3 representa os *value mapping* que serão utilizados como regras na criação dos *triggers*. Todos os dispositivos que suportam o protocolo SNMP devolvem os valores numéricos representados na Figura 5.3, onde o primeiro (*ifAdminStatus*) é utilizado para dar a informação sobre o estado de administração de uma respetiva porta do dispositivo e o segundo (ifOperStatus) dá informações sobre o estado operacional da porta.

SNMP interface status (ifAdminStatus)	1 ⇒ up 2 ⇒ down 3 ⇒ testing
SNMP interface status (ifOperStatus)	1 ⇒ up 2 ⇒ down 3 ⇒ testing 4 ⇒ unknown 5 ⇒ dormant 6 ⇒ notPresent 7 ⇒ lowerLayerDown

Figura 5.3 – Exemplo de Value mapping

5.4- Implementação do email no para envio dos alertas

Uma das formas de enviar alertas no Zabbix é através do email. Sendo assim, foi configurado o email para o envio desses alertas. Após reunião com o administrador de rede ficou definido que numa primeira fase os alertas serão enviados do email ”zabbix@max.uma.pt” para o email “zabbix@max.uma.pt”.

Foi criado um “Media types” com os dados que estão na Figura 5.4:

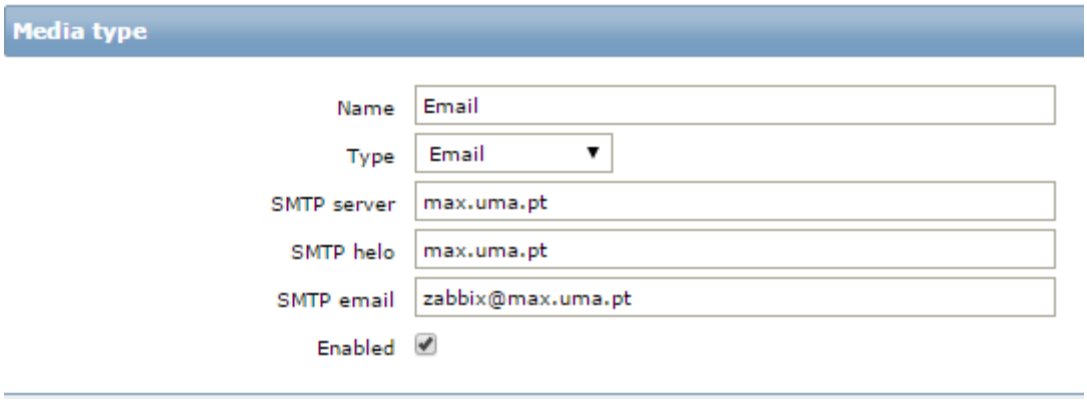


Figura 5.4 – Formulário para a criação de um serviço de alertas por email

5.5- Implementação da solução do cenário geral

Após a introdução do Router da Universidade da Madeira na ferramenta, através do protocolo SNMP e do template "SNMPv2_Interfaces" disponibilizado pelo Zabbix, é possível visualizar na ferramenta todas as portas existentes no Router, assim como os seus nomes associados. Com base no desenho para a solução do cenário geral descrito no subcapítulo 4.1- , foram implementados no Router, os triggers apresentados na Figura 5.5:

Severity	Name	Expression
Disaster	Admin Status was change Porta Externa(RCTS) Router	{gtuma.uma.pt:ifAdminStatus[GigabitEthernet0/3].diff(0)}=1
Disaster	Admin Status was change Porta Interna Router	{gtuma.uma.pt:ifAdminStatus[GigabitEthernet0/1].diff(0)}=1
High	Limit Traffic IN Porta Externa(RCTS) Router	{gtuma.uma.pt:ifInOctets[GigabitEthernet0/3].avg(4m)}>190M
High	Limit Traffic IN Porta Interna Router	{gtuma.uma.pt:ifInOctets[GigabitEthernet0/1].avg(4m)}>190M
High	Limit Traffic OUT Porta Externa(RCTS) Router	{gtuma.uma.pt:ifOutOctets[GigabitEthernet0/3].avg(4m)}>190M
High	Limit Traffic OUT Porta Interna Router	{gtuma.uma.pt:ifOutOctets[GigabitEthernet0/1].avg(4m)}>190M
Disaster	Operational status was changed Porta Externa(RCTS) Router	{gtuma.uma.pt:ifOperStatus[GigabitEthernet0/3].diff(0)}=1
Disaster	Operational status was changed Porta Interna Router	{gtuma.uma.pt:ifOperStatus[GigabitEthernet0/1].diff(0)}=1

Enable selected | Go (0)

Figura 5.5 – Implementação dos triggers no Router da Universidade da Madeira

Na Figura 5.5 podemos verificar que foi criado dois tipos de triggers, um relacionado com o estado da porta, em que verifica-se a existência de uma mudança de estado da mesma e o outro relacionado com o tráfego de entrada e saída na porta. O limite de tráfego da porta é de 200Mbps, logo criou-se um trigger em relação ao tráfego em que, se durante quatro minutos a média de tráfego de entrada ou saída for superior a 190Mbps, dispara um alerta.

Na *firewall* foi implementado os triggers em todas as portas. Estes foram implementados identicamente aos triggers do Router, onde a diferença está nos limites de tráfego para a emissão do alerta.

A Firewall contém dez portas, uma porta ligada ao Router e as outras nove ligadas à rede interna para a gestão das VLAN que têm acesso ao exterior. Todas as portas excetuando a porta que liga ao Router têm um limite de tráfego de 100Mbps, a porta que liga ao Router tem um limite de tráfego de 200Mbps. Sendo assim, as portas com limite de 100Mbps o trigger foi criado para emitir o alerta quando o tráfego médio de entrada ou saída durante quatro minutos for superior aos 95Mbps. Enquanto a porta com limite de tráfego a 200Mbps foi criado um trigger para emitir um alerta quando igualmente durante quatro minutos o tráfego médio de entrada ou saída for superior aos 195Mbps.

5.6- Implementação da solução entre edifícios

A implementação desta solução foi efetuada apenas na ligação entre o edifício da Penteada e o edifício da Reitoria, por esta ser a mais crítica. Esta solução foi implementada de forma simples. Os parâmetros desenhados no subcapítulo 4.2- , foram implementados com sucesso, como está representado na Figura 5.6.

Severity	Name	Expression	Status
Disaster	Admin Status was change Lig Penteada-Reitoria	{Bast_A_C16_4050:ifAdminStatus[RMON Port 09 on unit 1].diff(0)}=1	Enabled
High	Limit Traffic IN Conection Reitoria-Penteada	{Bast_A_C16_4050:ifInOctets[RMON Port 09 on unit 1].avg(5m)}>800M	Enabled
High	Limit Traffic OUT Conection Penteada-Reitoria	{Bast_A_C16_4050:ifOutOctets[RMON Port 09 on unit 1].avg(5m)}>800M	Enabled
Disaster	Operational status was changed on Lig Penteada-Reitoria	{Bast_A_C16_4050:ifOperStatus[RMON Port 09 on unit 1].diff(0)}=1	Enabled

Figura 5.6 – Implementação dos triggers ligação Penteada - Reitoria

5.7- Implementação da solução na rede wi-fi

A rede wi-fi é a rede mais crítica da Universidade da Madeira. Uma das redes mais utilizadas com reclamações dos utilizadores será uma prioridade do gestor em conhecer melhor esta rede. A implementação da solução da rede wi-fi teve algumas particularidades e problemas que serão descritos.

- Problema encontrado na implementação:
  Um problema inicial foi que após a introdução de um AP no Zabbix, verificou-se que o protocolo SNMP não estava a comunicar corretamente. Foi efetuado

alguns testes através da linha de comandos do servidor, com comandos relacionados com o protocolo SNMP. Um exemplo foi o comando "*snmpwalk –v2c public IP_host*" que serve para retornar toda a informação SNMP, mais precisamente os OIDs do equipamento. Foi testado com as várias versão do protocolo SNMP e o host não respondia.

- Solução para o problema:

  A solução passou por duas etapas.

  Após alguma investigação foi instalado no servidor as MIBs fornecidas pela Cisco, onde se encontrava o modelo dos APs existentes na Universidade da Madeira. Após este procedimento o host respondeu que não teria permissão para ler os OID do equipamento.

  Novamente, após alguma investigação, verificou-se que o problema possivelmente seria do "*snmp community*" um dos procedimentos seria alterar o "*snmp community*" que vem por defeito como "public". Após esta alteração a resposta do host foi totalmente positiva, fornecendo todos os OIDs do respetivo equipamento.

Após a resolução dos problemas encontrados nesta implementação, numa primeira fase de testes, foi introduzido 18 APs. Nestes APs foram implementados, com sucesso, os alertas que foram desenhados no subcapítulo 4.4- .

O Zabbix, como forma de organização, permite a criação de "Aplicações" dentro dos Templates, onde permite a criação de *Itens*. Como os APs têm todos a mesma função, foi então criado uma aplicação com o nome "Triggers para porta Ethernet e Wireless dos APs" onde dentro desta aplicação foram criados 4 *itens*. Dois para a porta wireless e dois para a porta *FastEthernet*. Estes são relacionados com o estado operacional e de administração das portas. Dentro dos *itens* foram criados os *triggers* relacionados com cada porta. Foram criadas expressões lógicas para alguns *triggers* como o exemplo da Figura 5.7. Será emitido um alerta, quando durante no mínimo três minutos, a porta FastEthernet se encontrar operacional e o *wireless* não se encontrar operacional, ou seja, existe tráfego na porta *Ethernet* e não existe qualquer emissão de ondas *radio* na porta *wireless*.

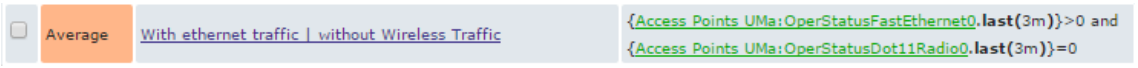


Figura 5.7 – Implementação trigger com condição no Access Point

Os templates utilizados para os APs, por serem templates genéricos aos equipamentos com suporte ao protocolo SNMP, não contêm a especificidade de retornar os valores dos utilizadores ativos nos APs, um parâmetro que poderá ser importante na resolução de um problema. Desta forma tiveram de ser criados novos *itens* nos *templates*. Para isso, o Zabbix permite a introdução dos *itens* com base num formulário onde é necessário a introdução correta do OID que pretendemos que seja retornado o valor e alguns parâmetros base de como queremos que sejam armazenados esses valores. Com base no *site* do fabricante, neste caso a Cisco, através do modelo do AP, foi retirada uma lista que se encontra no ftp "*ftp://ftp.cisco.com/pub/mibs/oid/CISCO-DOT11-ASSOCIATION-MIB.oid*", com todos os OIDs possíveis, existente no equipamento. Como podemos verificar na Figura 5.8, foi introduzido com sucesso no Zabbix o OID ""*cDot11ActiveWirelessClients*" - "*1.3.6.1.4.1.9.9.273.1.1.2.1.1*"".

Nesta fase o número máximo de utilizadores ativos, para a emissão de um alerta ficou definido em 20, este valor poderá ser alterado após os testes.

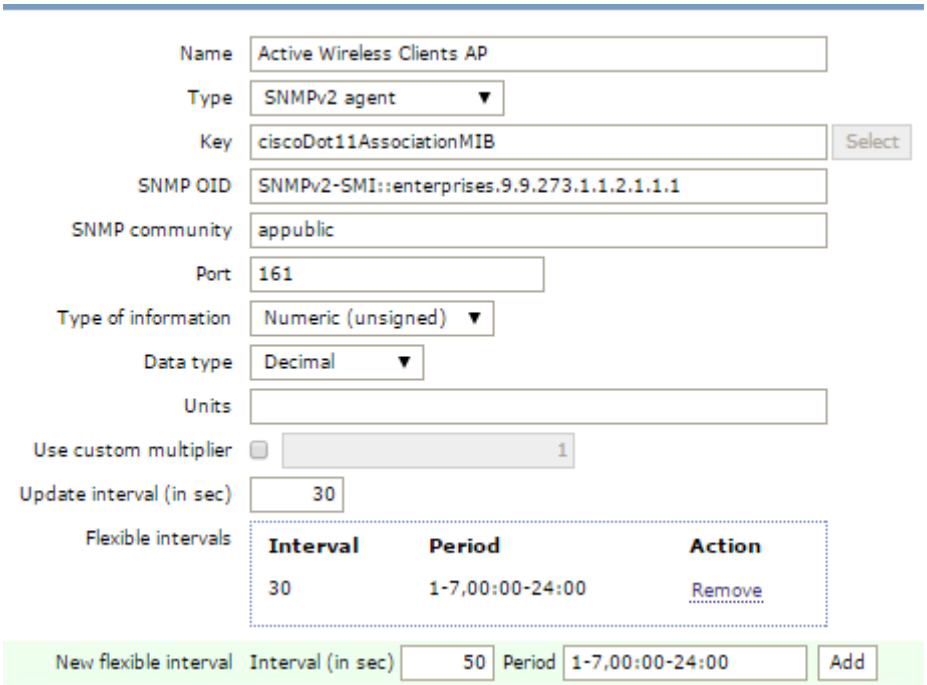


Figura 5.8 – Formulário para a criação de um Item

5.8- Implementação da solução na arquitetura lógica das VLANs

Devido às restrições descritas no início deste capítulo este cenário não foi implementado por completo. Contudo, através do protocolo SNMP utilizado para a recolha de informações sobre os equipamentos, é possível uma monitorização das VLAN em todos os equipamentos adicionados ao Zabbix, gerando gráficos de tráfego divididos por VLAN. A Figura 5.9. mostra um dos Switchs Core do Bastidor principal, onde é possível verificar o tráfego de qualquer uma das VLAN configuradas no equipamento.

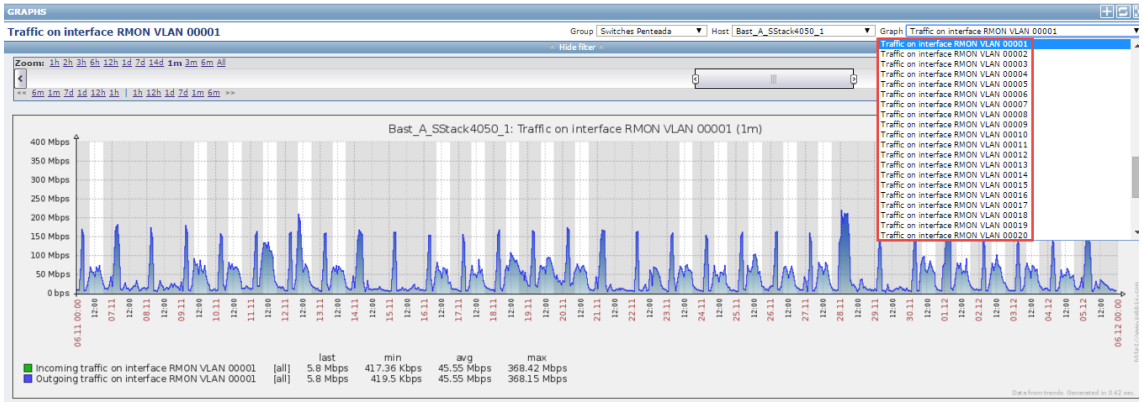


Figura 5.9 – Visualização do tráfego das VLAN configuradas no equipamento

5.9- Implementação da solução no bastidor Central do edifício da Penteada

A implementação desta solução teve como base, o desenho descrito no subcapítulo 4.3- . Todos os parâmetros anteriormente descritos foram implementados com sucesso.

Após reunião com o gestor de rede ficou decidido que os alertas seriam configurados para serem emitidos quando as ligações atingissem 80% de ocupação. A Figura 5.10 apresenta os *triggers* configurados para ir de encontro aos objetivos traçados neste projeto, dando a conhecer o tráfego existente no backbone, o que até à data era desconhecido para o gestor de rede.

Severity	Name	Expression	Status
High	Admin status was changed in Lig Bast_A - Bast_B	{BAST_A_C1_4050:ifAdminStatus[RMON Port 21 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_C	{BAST_A_C1_4050:ifAdminStatus[RMON Port 24 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_CO	{BAST_A_C1_4050:ifAdminStatus[RMON Port 27 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_D	{BAST_A_C1_4050:ifAdminStatus[RMON Port 20 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_E	{BAST_A_C1_4050:ifAdminStatus[RMON Port 05 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_F - PORTA3	{BAST_A_C1_4050:ifAdminStatus[RMON Port 03 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_F - PORTA4	{BAST_A_C1_4050:ifAdminStatus[RMON Port 04 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_G	{BAST_A_C1_4050:ifAdminStatus[RMON Port 25 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_H	{BAST_A_C1_4050:ifAdminStatus[RMON Port 26 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_I	{BAST_A_C1_4050:ifAdminStatus[RMON Port 22 on unit 1].diff(0)}=1	Enabled
High	Admin status was changed in Lig Bast_A - Bast_J	{BAST_A_C1_4050:ifAdminStatus[RMON Port 19 on unit 1].diff(0)}=1	Enabled
High	Admin Status was change Porta Ligação Stack BastA	{BAST_A_C1_4050:ifAdminStatus[RMON Port 07 on unit 1].diff(0)}=1	Enabled
Average	Limit Traffic IN Conection Bast_B - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 21 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_C - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 24 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_CO - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 27 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_D - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 20 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_E - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 05 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_F - Bast_A - PORTA3	{BAST_A_C1_4050:ifInOctets[RMON Port 03 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_F - Bast_A - PORTA4	{BAST_A_C1_4050:ifInOctets[RMON Port 04 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_G - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 25 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_H - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 26 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_I - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 22 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Conection Bast_J - Bast_A	{BAST_A_C1_4050:ifInOctets[RMON Port 19 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic IN Porta Ligação Stack BastA	{BAST_A_C1_4050:ifInOctets[RMON Port 07 on unit 1].avg(4m)}>500M	Enabled
Average	Limit Traffic OUT Conection Bast_A - Bast_B	{BAST_A_C1_4050:ifOutOctets[RMON Port 21 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic OUT Conection Bast_A - Bast_C	{BAST_A_C1_4050:ifOutOctets[RMON Port 24 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic OUT Conection Bast_A - Bast_CO	{BAST_A_C1_4050:ifOutOctets[RMON Port 27 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic OUT Conection Bast_A - Bast_D	{BAST_A_C1_4050:ifOutOctets[RMON Port 20 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic OUT Conection Bast_A - Bast_E	{BAST_A_C1_4050:ifOutOctets[RMON Port 05 on unit 1].avg(4m)}>800M	Enabled
Average	Limit Traffic OUT Conection Bast_A - Bast_F - PORTA3	{BAST_A_C1_4050:ifOutOctets[RMON Port 03 on unit 1].avg(4m)}>800M	Enabled

Figura 5.10 – Implementação dos triggers no backbone do edifício da Penteada

Capítulo 6- Testes e Resultados

Neste capítulo serão apresentados os testes e os resultados adquiridos após a implementação dos cenários apresentados.

Com base nos objetivos definidos no primeiro capítulo, e nos processos que os cenários criados para a solução foram passando, até à fase de implementação, nomeadamente a contextualização, análise, desenho e implementação, será apresentado os testes e os seus resultados dos cenários que permitiram retirar conclusões sobre os problemas descritos no primeiro capítulo.

Por ser uma das prioridades do gestor de rede da Universidade da Madeira, o cenário da rede wi-fi foi o mais investigado para podermos obter resultados concretos da causa das reclamações por parte dos utilizadores desta rede.

Para uma melhor análise dos gráficos que irão ser apresentados de seguida, o Zabbix permite colocar um fundo branco nas horas em que a instituição está realmente em maior produção. Neste caso foi colocado um horário de produção das 09h00 até às 18h00, de segunda a sexta-feira.

As legendas das figuras apresentadas neste capítulo, contêm o intervalo de tempo da captura dos dados recolhidos para a monitorização, com a seguinte nomenclatura: M-meses, d-dias, h-horas, m-minutos.

6.1- Testes e Resultados do cenário geral

Nesta secção os testes efetuados ao cenário geral foram com base nos problemas e na necessidade do gestor de rede conhecer o tráfego e estado dos equipamentos que representam este cenário, nomeadamente o Router e a Firewall. Como foi descrito no subcapítulo 3.2.1- , estes são equipamentos de elevada importância para a UMa. Os testes e resultados apresentam, primeiro, uma análise ao Router e, seguidamente, uma análise à Firewall.

6.1.1- Testes e Resultados ao Router

Após a instalação do Router na ferramenta foi analisado por um período de 2 meses o tráfego semanal da ferramenta. A Figura 6.1 representa um mês de funcionamento do Router relativamente à porta que liga à rede interna. Pode-se analisar um padrão no

tráfego de entrada e saída durante este período de tempo, em que verifica-se que existe dois picos diários durante o período de produção (representado com um fundo branco) nos dias úteis. A Figura 6.2, é efetuado uma diminuição no intervalo de tempo em análise para apenas sete dias. Pode-se verificar melhor o padrão existente sendo na hora de almoço o período de diminuição do tráfego.

Embora tenha havido um "pico" em que o tráfego esteve acima do alerta definido pelo *trigger*, este não excedeu o tempo de permanência de 4 minutos acima dos 190 Mbps, o que, seguindo o que foi desenhado e implementado na solução deste cenário, não foi emitido nenhum alerta devido ao tempo de permanência ser menor que 4 minutos.

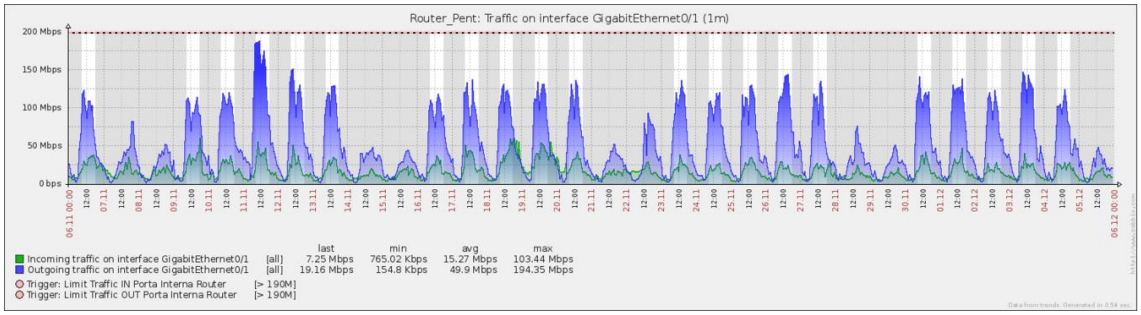


Figura 6.1 – Gráfico do tráfego de *in/output* na porta que liga à rede interna no Router (1M)

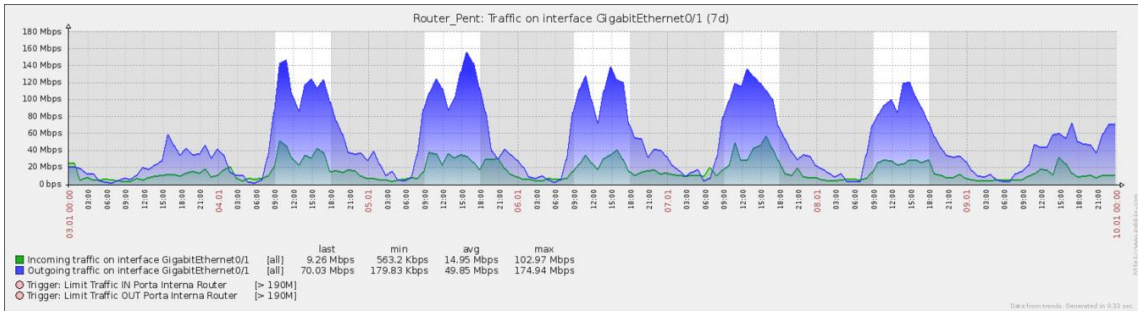


Figura 6.2 - Gráfico do tráfego de *in/output* na porta que liga à rede interna no Router (7d)

6.1.2- Testes e resultados à Firewall

Os testes à *firewall* foram efetuados com o mesmo intervalo de tempo definido anteriormente no Router de um mês. Neste cenário de rede pode-se analisar e comparar o tráfego das VLAN.

Conectados à Firewall estão as duas VLAN mais utilizadas e mais distintas, a VLAN dos alunos e a VLAN dos docentes e funcionários onde também estão alocados os servidores.

A Figura 6.3 representa a VLAN dos docentes e a Figura 6.4 representa a VLAN dos alunos. Pode-se verificar uma grande diferença de tráfego entre estas duas VLAN, podendo dizer através das médias (avg) apresentadas nas figuras, que a VLAN dos alunos utiliza o dobro de tráfego, que a VLAN dos docentes. Por vezes, a VLAN dos alunos chega a atingir os limites de tráfego permitido na porta da firewall, que são apenas 100Mbps.

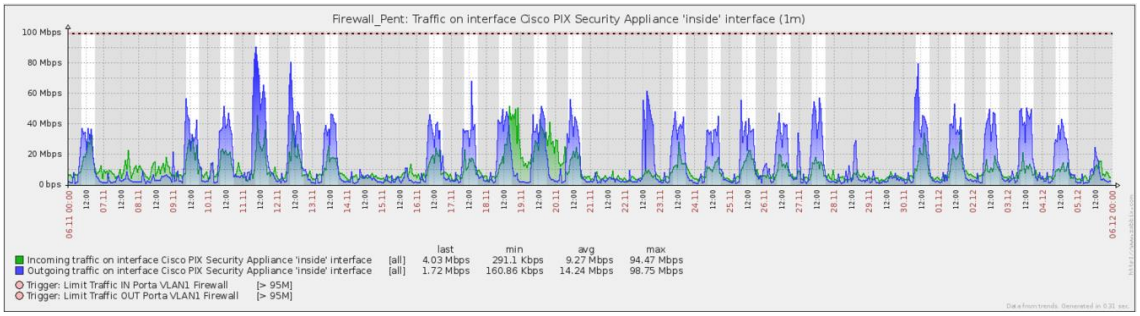


Figura 6.3 – Gráfico do tráfego de in/output na porta que liga à VLAN1 na Firewall (1M)

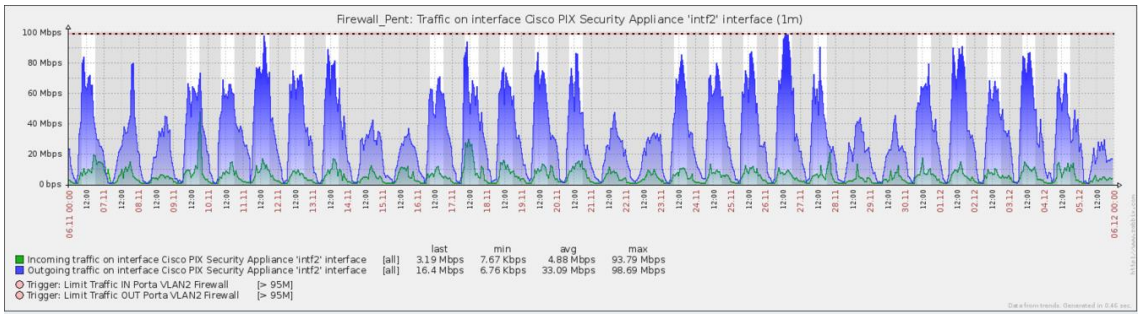


Figura 6.4 – Gráfico do tráfego de in/output na porta que liga à VLAN2 na Firewall (1M)

Em suma, pode-se concluir que o Router, a Firewall e as ligações, não estão com sobrecarga diária. Se existir alguma lentidão no lado dos utilizadores nas ligações ao exterior, estas poderão ser de algum equipamento que esteja a ser utilizado até à chegada ao Router ou o fornecedor do serviço de internet não tem resposta suficiente para os pedidos dos utilizadores da Universidade da Madeira.

6.2- Testes e Resultados da solução na rede wi-fi

Os testes a este cenário foram com base na resolução dos problemas de lentidão e o desconhecimento do tráfego existente nos equipamentos e ligações que constituem esta rede, nomeadamente os APs, por parte do gestor de rede.

Numa primeira fase dos testes foi analisado os gráficos relativamente ao tráfego nos equipamentos e ligações, onde surpreendentemente, foi verificado que em todos os APs instalados o seu tráfego nunca atingia limites. Pelo contrário muitos deles nem chegavam ao máximo de 2Mbps por dia. Apenas o AP situado na biblioteca tinha uma média diária de 7.5Mbps. Podemos concluir que os APs não estão com sobrecarga de tráfego.

Como desenho desta solução, descrita no subcapítulo 4.4- , decidiu-se verificar o número de utilizadores ativos em cada AP. Após a implementação desta solução verificou-se que existia um número elevado de utilizadores ativos nos APs, atingindo muitas vezes 100 utilizadores ativos em simultâneo.

Nas Figura 6.5 e Figura 6.6 podemos verificar as situações descritas acima. Onde na Figura 6.5 está representado dois APs situados no piso -2 junto a salas de aulas, na parte superior da Figura 6.5 está representado o tráfego de entrada e saída pela porta Radio(Wireless), na parte inferior da Figura 6.5 está representado o número de utilizadores ativos. Os gráficos estão todos no mesmo intervalo de tempo de três dias semanais.

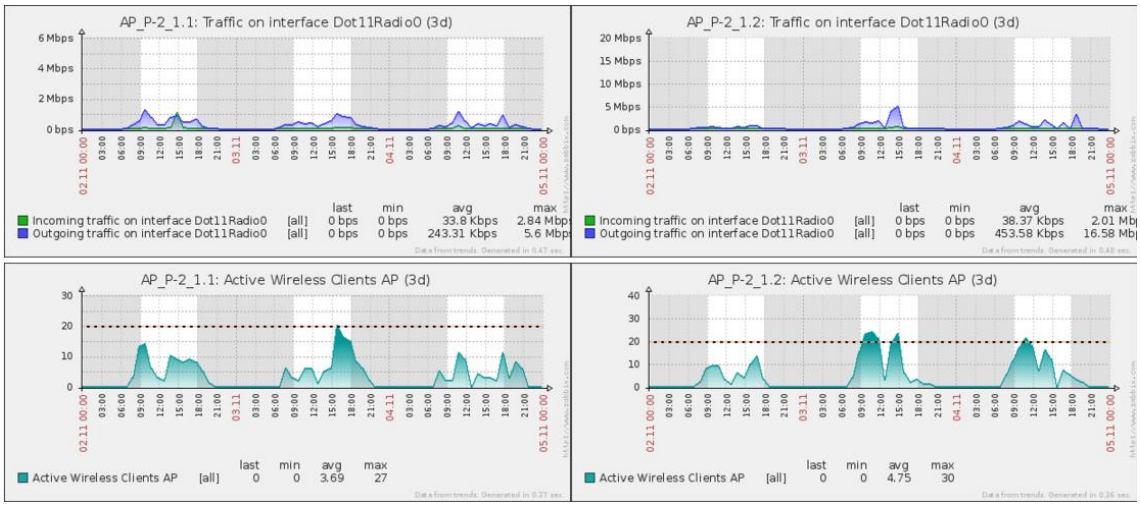


Figura 6.5 – Vista comparativa dos gráficos de dois APs relação Tráfego-Clientes ativos (3d)

Na Figura 6.6, está representado dois APs situados em pontos onde possivelmente seriam os pontos com maior utilização. No lado esquerdo está representado o AP situado na biblioteca e o do lado direito está representado o AP situado na Cantina da Universidade. Igualmente na parte superior está representado o tráfego de entrada e saída na porta Radio(wireless) e na parte inferior o número de utilizadores ativos em simultâneo.

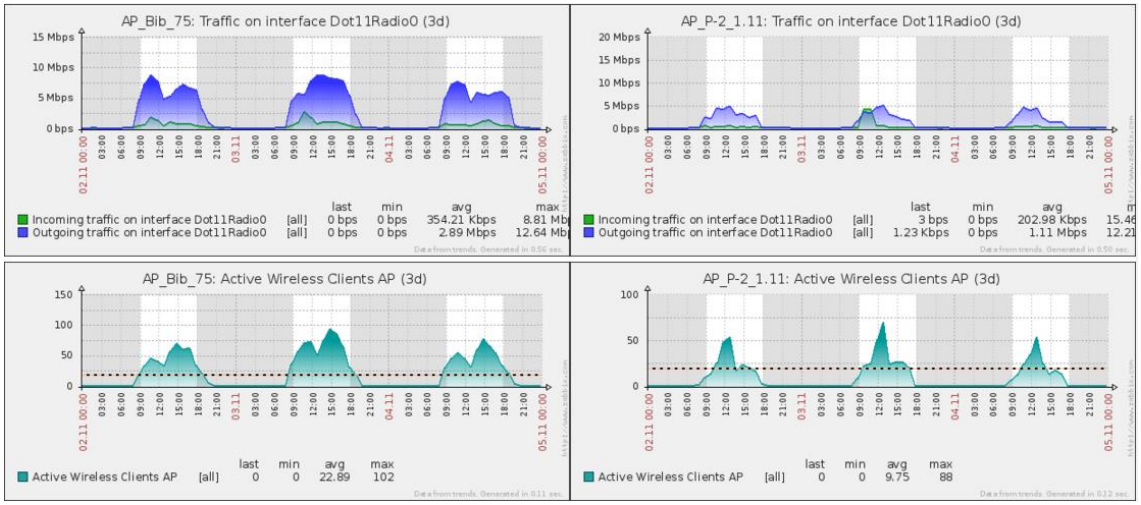


Figura 6.6 Vista comparativa dos gráficos de dois APs relação Tráfego-Clientes ativos (3d)

Pode-se verificar que mesmo o número de utilizadores ativos em simultâneo estando elevado, o tráfego continua não atingindo os limites. Nos gráficos acima podemos ainda, verificar uma série de contradições relacionando o tráfego com o número de utilizadores ativos. É possível verificar subidas de tráfego em simultâneo com a subida do número de utilizadores, como com a subida de utilizadores temos uma descida no tráfego.

Após várias análises e testes detalhados em vários APs, e através de alguma investigação, conclui-se que o problema está no modelo do AP e no número de utilizadores ativos em simultâneo.

Exemplificando o que está escrito acima, temos que, os APs utilizados na UMa fazem uma divisão de tráfego dependendo do número de utilizadores ligados ao AP, isto é, imaginemos que o limite de tráfego de um AP é 54Mbps em *half-duplex*, e estão

ligados ao AP 20 utilizadores, mas apenas 2 desses utilizadores estão realmente a usar a internet e os outros apenas ligaram o computador e como já está por defeito a ligação a uma rede wi-fi, este fica conectado ao AP. Por sua vez, o AP não consegue dividir os 54Mbps pelos dois utilizadores que realmente precisam de internet, dividindo assim 1.35Mbps *half-duplex* para cada um dos 20 utilizadores.

Atualmente, um número elevado de pessoas têm um smartphone, e outras têm igualmente um tablet e um computador. Seguindo esta realidade na UMa, no AP da biblioteca onde possivelmente estão 30 alunos, se cada um tiver o seu computador, o seu smartphone e se 10 desses alunos ainda têm outro equipamento ligado ao AP mesmo sem estar a navegar na Internet, isto dá um total de 70 utilizadores num AP enquanto possivelmente apenas 25 estão realmente a necessitar da internet.

Esta situação apenas seria possível com APs mais modernos onde consigam fazer a gestão do tráfego dividindo o tráfego pelos utilizadores que realmente estão a navegar na internet.

6.3- Testes e Resultados à ferramenta Zabbix

Após a implementação dos dispositivos descritos no subcapítulo da implementação dos cenários e no início da fase de testes e apresentação de resultados, foi detetada uma ligeira lentidão na navegação da ferramenta e 6 a 8 vezes ao dia era disparado um alerta dizendo que a utilização do disco I/O, estava acima dos 80%. Através do agente instalado no servidor Zabbix, foi produzido gráficos, onde pode-se analisar que o disco estava sempre acima dos 80% chegando muitas vezes acima dos 90%.

A situação acima referida foi reportada ao administrador de rede onde prontamente fez uma migração do servidor Zabbix para uma máquina virtual situada nos servidores Blades com um CPU “Intel® Xeon® Processor E5-2620 - 15M Cache, 2.00 GHz 6 Cores” 60GB de disco e 8GB de RAM. Uma limitação deste projeto que só foi detetado nesta fase é que o sistema operativo instalado inicialmente foi de 32bit o que com esta evolução o sistema não reconhece mais do que 4GB de memória RAM.

Após esta evolução, o sistema aumentou exponencialmente a velocidade. Os tempos de resposta na deteção de novos *hosts* e na adição de novos *itens* nos *templates* eram

de um a dois minutos passaram para menos de um minuto. A utilização do disco como podemos analisar na Figura 6.7 diminuiu para 20% e o processador para menos de 5%.

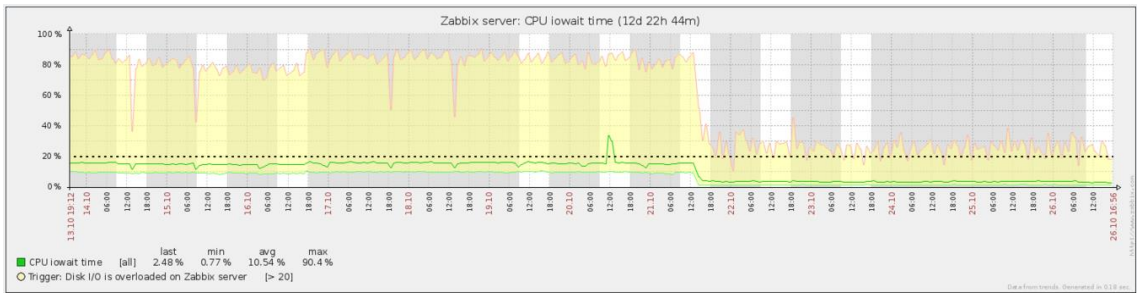


Figura 6.7 – Gráfico com a utilização do disco e CPU do Zabbix Server (12d22h44m)

Capítulo 7- Conclusões e trabalhos futuros

Um fator importante de todo o desenvolvimento deste projeto, foi a necessidade de produzir um estudo inicial das características da rede da UMa. Esta foi uma tarefa complexa devido às grandes dimensões da rede. Demorou imenso tempo, foram efetuadas várias reuniões com o gestor de rede. No entanto, este trabalho inicial possibilitou a perceção e a compreensão da estrutura e o funcionamento da rede permitindo um levantamento de necessidades e problemas existentes na área de gestão e monitorização da rede e serviços da Universidade da Madeira.

Salienta-se o facto de não ter sido possível testar todas as aplicações selecionadas para a realização deste projeto na íntegra, ficando este trabalho apenas pela utilização de Máquinas Virtuais na comparação das ferramentas, tendo-se baseado a escolha, essencialmente no estudo acima referido no subcapítulo 3.3- e, tendo em conta a documentação existente sobre cada ferramenta e tentando sempre assegurar a ferramenta com a melhor relação custo-benefício. Esta tarefa não foi simples, devido ao facto de abranger a análise e comparação de várias funcionalidades de um conjunto de ferramentas, para que fosse possível a seleção da ferramenta que mais se adapte à realidade da UMa.

De modo resumido, destaca-se o facto de antes de ser implementada esta solução, afirma-se que apenas existia na UMa uma solução de gestão e monitorização com recurso a uma ferramenta no Centro de Competências de Ciências Exatas e da Engenharia (CCCEE). Esta serviu de apoio à fase inicial deste projeto.

A adição de um sistema de envio de alertas por SMS, além do envio por e-mail já configurado, assim como a adição de um ZabbixProxy no edifício da reitoria e no edifício da SASUMA, como descrito na arquitetura da solução, no sentido de alcançar uma monitorização de toda a rede da Universidade da Madeira, constituem os principais trabalhos futuros. No sentido de aprimorar, é importante a introdução no sistema de monitorização os servidores existentes na instituição. Estes não foram introduzidos na ferramenta devido ao facto de ter sido dado prioridade aos sistemas mais críticos relatados pelo gestor de rede.

Com base nos futuros dados que serão recolhidos pela ferramenta, seria igualmente uma melhoria, um novo ajustamento dos limites de tráfego para a geração de *triggers*.

A informação adquirida no desenvolvimento deste projeto, permite afirmar que uma estratégia de gestão preventiva e corretiva das tecnologias de informação é um ponto crucial para obter uma rede sólida e fiável

Em suma, conclui-se que os objetivos definidos neste projeto foram alcançados de forma positiva. A Universidade da Madeira ficou dotada com um sistema de monitorização, que corresponde aos requisitos dos administradores de rede.

Capítulo 8- Referências

[1] F. Boavida, M. Bernardes, e P. Vapi, *Administração de Redes Informáticas*, 2ª ed. FCA.

[2] J. F. Kurose e Keith W. Ross, *Computer Networking: ATop-Down Approach*, 6ª ed. Pearson.

[3] «RFC 2570 - Introduction to Version 3 of the Internet-standard Network Management Framework». [Em linha]. Disponível em: https://tools.ietf.org/html/rfc2570. [Acedido: 28-Out-2015].

[4] «RFC 1441 - Introduction to version 2 of the Internet-standard Network Management Framework». [Em linha]. Disponível em: https://tools.ietf.org/html/rfc1441. [Acedido: 18-Out-2015].

[5] K. McCloghrie, K. McCloghrie, J. Schoenwaelder, e D. Perkins, «Structure of Management Information Version 2 (SMIv2)». [Em linha]. Disponível em: https://tools.ietf.org/html/rfc2578. [Acedido: 18-Out-2015].

[6] «RFC 2580 - Conformance Statements for SMIv2». [Em linha]. Disponível em: https://tools.ietf.org/html/rfc2580. [Acedido: 28-Out-2015].

[7] «RFC 2578 - Structure of Management Information Version 2 (SMIv2)». [Em linha]. Disponível em: https://www.ietf.org/rfc/rfc2578.txt. [Acedido: 31-Out-2015].

[8] «RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II». [Em linha]. Disponível em: https://www.ietf.org/rfc/rfc1213.txt. [Acedido: 28-Out-2015].

[9] «What Is SNMP?: Simple Network Management Protocol (SNMP); Services for Macintosh». [Em linha]. Disponível em: https://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx. [Acedido: 17-Out-2015].

[10] P. Goyal, R. Mikkilineni, e M. Ganti, «FCAPS in the Business Services Fabric Model».

[11] E. Monteiro e F. Boavida, *Engenharia de Redes Informáticas*, 7ª ed. FCA.

[12] «What is a Virtual Local Area Network (VLAN)? - Definition from Techopedia», *Techopedia.com*. [Em linha]. Disponível em: http://www.techopedia.com/definition/4804/virtual-local-area-network-vlan. [Acedido: 28-Jul-2015].

[13] «Nagios Core. Nagios Open Source Project.» [Em linha]. Disponível em: https://www.nagios.org/. [Acedido: 29-Nov-2015].

[14] «Xposé : Supervision - Nagios». [Em linha]. Disponível em: http://www-igm.univ-mlv.fr/~dr/XPOSE2004/nchaveron/Nagios.html. [Acedido: 29-Nov-2015].

[15] «FAQ | Icinga». [Em linha]. Disponível em: https://www.icinga.org/resources/faq/. [Acedido: 04-Dez-2015].

[16] «Icinga - Sistema de Monitorização de Servidores», *Alojamento Web*. .

[17] «Architecture | Icinga». [Em linha]. Disponível em: https://www.icinga.org/icinga/icinga-1/architecture/. [Acedido: 07-Dez-2015].

[18] «Distributed Monitoring | Icinga». [Em linha]. Disponível em: https://www.icinga.org/icinga/icinga-2/distributed-monitoring/. [Acedido: 04-Dez-2015].

[19] J. W. in P. Spotlight, A. 17, 2010, e 4:02 AM PST // jlwallen, «Review: Zenoss network monitoring tool», *TechRepublic*. [Em linha]. Disponível em: http://www.techrepublic.com/blog/product-spotlight/review-zenoss-network-monitoring-tool/. [Acedido: 12-Fev-2015].

[20] «Zenoss Community - Open Source Network Monitoring and Systems Management». [Em linha]. Disponível em: http://www.zenoss.org/. [Acedido: 03-Jan-2016].
[21] «O que é Zabbix? ferramenta de monitoramento de redes». [Em linha]. Disponível em: http://www.4linux.com.br/o-que-e-zabbix. [Acedido: 23-Nov-2015].
[22] «Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution». [Em linha]. Disponível em: http://www.zabbix.com/functionality.php. [Acedido: 24-Nov-2015].
[23] «Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution». [Em linha]. Disponível em: http://www.zabbix.com/distributed_monitoring.php. [Acedido: 24-Nov-2015].
[24] «Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution». [Em linha]. Disponível em: http://www.zabbix.com/requirements.php. [Acedido: 23-Nov-2015].
[25] «Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution». [Em linha]. Disponível em: http://www.zabbix.com/zabbix_agent.php. [Acedido: 24-Nov-2015].
[26] O. Marik e S. Zitta, «Comparative analysis of monitoring system for data networks», em *2014 International Conference on Multimedia Computing and Systems (ICMCS)*, 2014, pp. 563–568.
[27] «Zabbix Manual [Zabbix Documentation 2.4]». [Em linha]. Disponível em: https://www.zabbix.com/documentation/2.4/manual. [Acedido: 21-Nov-2015].
[28] Nagios Enterprises, «Nagios XI - Hardware Requirements». .
[29] «System Requirements - HowTos - Icinga Wiki». [Em linha]. Disponível em: https://wiki.icinga.org/display/howtos/System+Requirements. [Acedido: 03-Jan-2016].
[30] Zenoss, «Zenoss Core Installation and Upgrade». .
[31] «6 Templates [Zabbix Documentation 2.4]». [Em linha]. Disponível em: https://www.zabbix.com/documentation/2.4/manual/config/templates. [Acedido: 17-Jan-2016].

Capítulo 9- Anexos

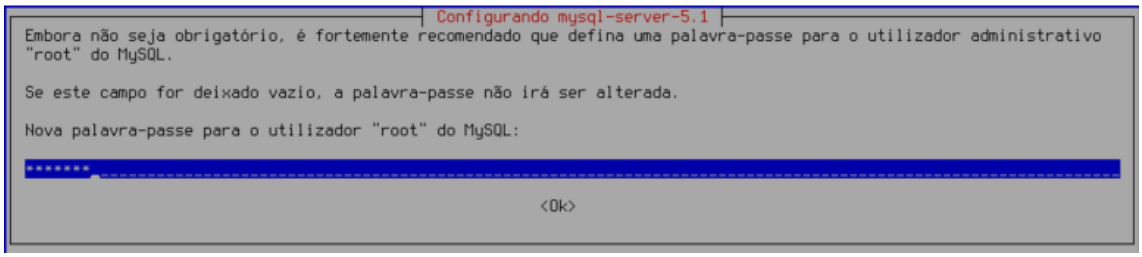
9.1- Instalação do Zabbix 2.4 no Debian 7

Os procedimentos para a instalação foram os seguintes:

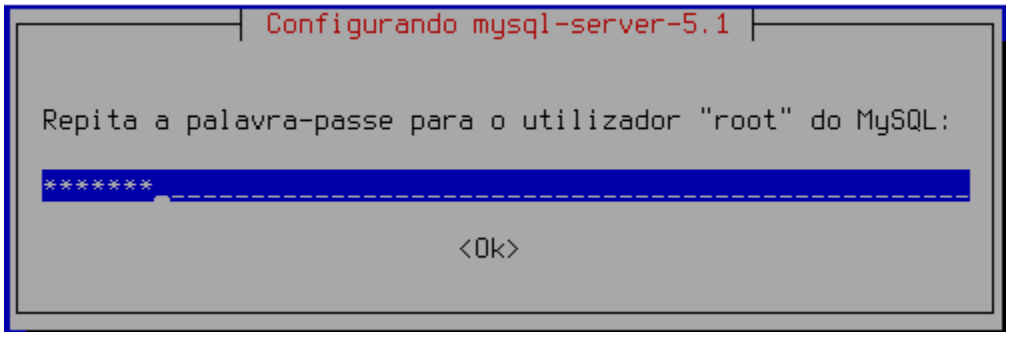
1. Introduzir na linha de comandos:

#apt-get install zabbix-server-mysql zabbix-frontend-php

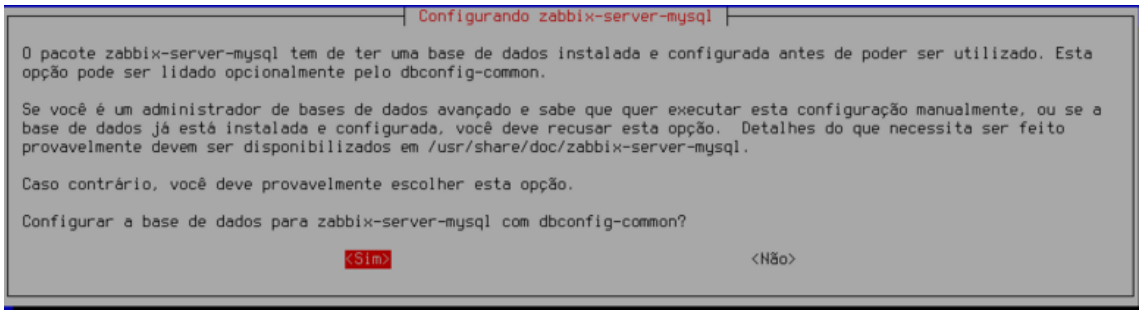
2. Introduzir a senha de root do MySQL



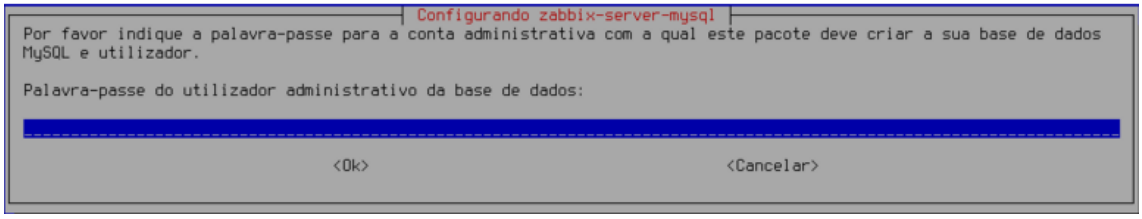
3. Repetir introdução da senha de root



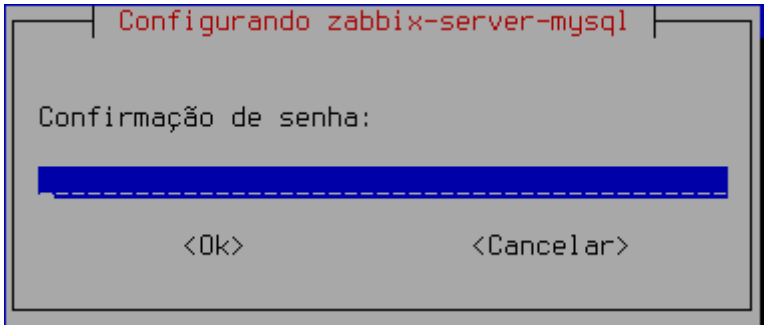
4. Utilizar o dbconfig-common para configurar o zabbix-server-mysql



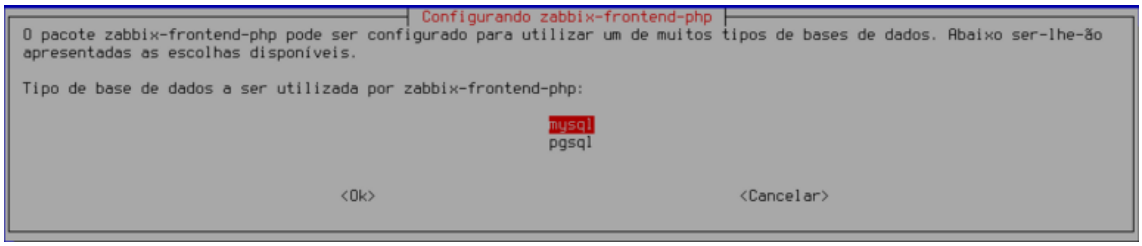
5. Escrever a senha do MySQL



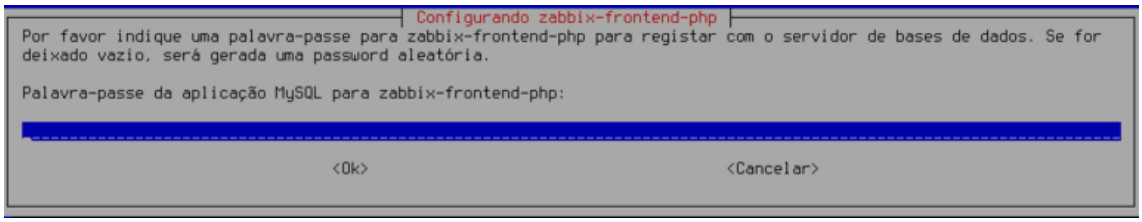
6. Repetir a senha



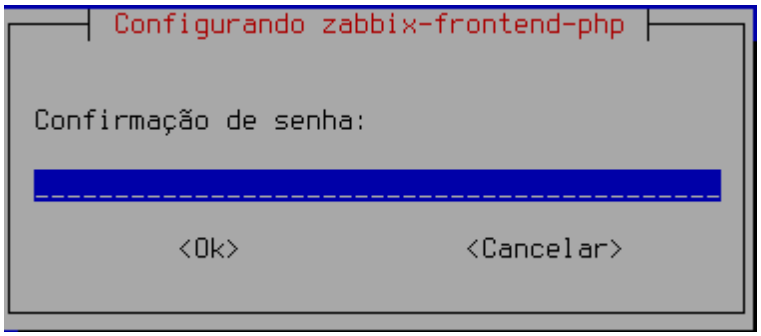
7. Escolher o Mysql como SGBD(Sistema Gestor de Base de Dados)



8. Introduzir a senha para o frontend PHP do Zabbix



9. Repetir a senha



A Intalação do MySQL, Zabbix e Apache2 foi concluída, agora temos de realizar alguns ajustes no PHP

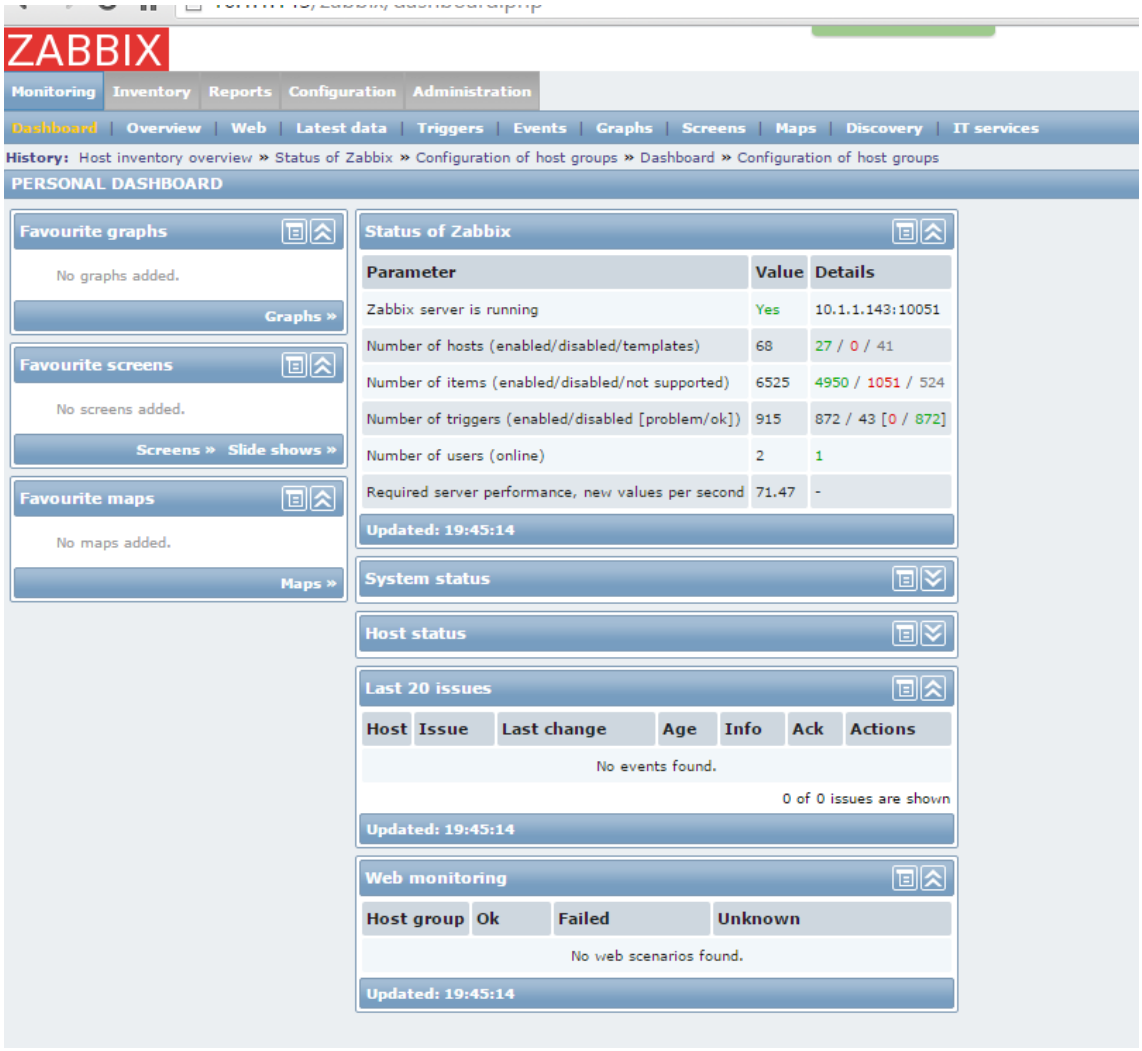
10. Introduzir o comando "nano /etc/apache2/conf.d/zabbix" e alterar os valores para:

```
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value date.timezone Europe/Lisbon
```

11. Com todas as configurações realizadas, temos de reiniciar os serviços, Zabbix Server, Zabbix Agent e Apache2 com os seguintes comandos:
    - Zabbix server:
        - /etc/init.d/zabbix-server restart
    - Zabbix Agent
        - /etc/init.d/zabbix-agent restart
    - Apache2
        - service apache2 restart
12. Após reiniciar os serviços, abrimos o browser e escrevemos o seguinte endereço http://ip_do_servidor/zabbix irá mostrar a seguinte figura:

13. Agora é seguir as instruções simples solicitadas e no fim será apresentado o seguinte ecrã:

14. Após introduzir as credenciais, Username “Admin” e Password “zabbix” será apresentado um Dashboad em pleno funcionamento.



A instalação da ferramenta Zabbix está finalmente concluída.

Nota: Os arquivos de configuração do zabbix encontram-se em /etc/zabbix.