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

PROJETO DE MESTRADO

Andreia Filipa Camacho Marques
MESTRADO EM ENGENHARIA INFORMÁTICA

UNIVERSIDADE da MADEIRA
A Nossa Universidade
www.uma.pt

Julho | 2015

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

PROJETO DE MESTRADO

Andreia Filipa Camacho Marques

MESTRADO EM ENGENHARIA INFORMÁTICA

ORIENTADOR

Lina Maria Pestana Leão de Brito

CO-ORIENTADOR

Eduardo Miguel Dias Marques

UNIVERSIDADE da MADEIRA

Desenho e implementação de uma plataforma integrada para monitorização e gestão de uma rede de um departamento da UMa

Andreia Filipa Camacho Marques
(Licenciada)

Tese submetida à Universidade da Madeira para a
Obtenção do Grau de Mestre em Engenharia Informática

Portugal – Madeira

Julho 2015

Resumo

A área da gestão de sistemas e redes tem vindo a alcançar um papel crucial em todas as áreas das Tecnologias de Informação (TI). Com o constante desenvolvimento das redes, em dimensão, inovação tecnológica ou em heterogeneidade, o processo de gestão e monitorização destes sistemas tornou-se cada vez mais exigente e complexo, forçando diversas organizações a investir na implementação ou aquisição de algum *software* de apoio para os gestores de redes.

Com o presente trabalho, pretende-se implementar uma solução integrada para permitir uma gestão preventiva e correctiva dos sistemas da rede informática de um dos departamentos da Universidade da Madeira, denominado por Centro de Competências de Ciências Exactas e da Engenharia (CCCEE).

A abordagem a essa solução começa por dar a conhecer alguns dos princípios mais importantes das tradicionais arquitecturas de gestão de redes, e por apresentar um modelo de referência que disponibiliza um conjunto de boas práticas para a gestão de TI.

O trabalho continua com o estudo das características da rede informática existente nas instalações do CCCEE, identificando-se não só as reais necessidades na área da gestão e monitorização das TI, como também os principais problemas que a nova solução deveria intervir. A partir destes dados e através de uma análise a um conjunto de ferramentas de gestão e monitorização de redes, selecionou-se a que mais se adequava à realidade do CCCEE.

Este trabalho terminou com a monitorização e gestão, contínua e eficiente, das tecnologias de informação do CCCEE, através da implementação da arquitectura de uma solução integrada, de acordo com requisitos e políticas do CCCEE.

Palavras-chave: gestão e monitorização de redes, gestão e monitorização de serviços, ferramentas de gestão, solução integrada de gestão

Abstract

The area of systems and network management has achieved a crucial role in all areas of the Information Technology (IT). With the constant development of the network, regarding its dimension, technological innovation or heterogeneity, the process of managing and monitoring these systems has become increasingly demanding and complex, forcing many organizations to invest in the implementation or acquisition of some software to support the network managers.

With this work, we intend to implement an integrated solution, to enable preventive and corrective management of computer network systems, of one of the departments of the University of Madeira, denominated by Centro de Competências de Ciências Exactas e da Engenharia (CCCEE).

The approach to this solution begins with the description of some of the most important principles of traditional network management architectures, and with the presentation of a reference model that provides a set of best practices for IT management.

This work continues with the study of the features of the network installed in CCCEE facilities, identifying not only the real needs in the area of management and monitoring of IT, but the main problems that the new solution should intervene as well. Based on this and by analyzing a set of network management and monitoring tools, we have selected the one most suitable to the CCCEE reality.

This work ends with a continuous and efficient monitoring and management of information technology of the CCCEE, through the implementation of the architecture of an integrated solution, according to CCCEE's requirements and policies.

Key words: networks management and monitoring, services management and monitoring, management tools, integrated management solutions

Agradecimentos

A concretização deste Projecto de Mestrado foi unicamente possível graças à colaboração e ao contributo, de um conjunto pessoas, às quais gostaria de transmitir o meu agradecimento e reconhecimento, nomeadamente:

À Prof. Lina Brito, minha orientadora, e ao Prof. Eduardo Marques, meu co-orientador, que foram os principais responsáveis por eu ter conseguido concluir este projecto. Agradeço a constante orientação, contributos, motivação, paciência e disponibilidade demostrada durante todo este tempo.

Um agradecimento especial à minha família, em particular aos meus pais e à minha irmã. Agradeço pelo constante apoio (e paciência), não só nesta fase mas, principalmente, em todo o meu percurso universitário.

E, por fim, não menos importante, um agradecimento a todos aqueles que, de algum modo, directa ou indirectamente, colaboraram para a realização deste projecto.

A todos, o meu MUITO OBRIGADA!!!

Conteúdo

Resumo v

Abstract vii

Agradecimentos ix

Conteúdo xi

Lista de Figuras xiii

Lista de Tabelas xiv

Acrónimos xv

1. **Introdução** 17

1.1. Contextualização 17

1.2. Problema 18

1.3. Objectivos da Tese 19

1.4. Organização da Tese 19

2. **Estado da Arte** 21

2.1. Introdução 21

2.2. Gestão e Monitorização de Redes 22

2.2.1. Modelo FCAPS 23

2.2.2. Arquitecturas de Gestão OSI e TMN 25

2.2.3. Arquitectura de Gestão da Internet 28

2.3. Modelo ITIL 30

2.4. Ferramentas de Gestão de Redes 34

2.4.1. Selecção e Descrição das Ferramentas 35

2.5. Conclusão 42

3. **Gestão de Sistemas e Serviços do CCCEE** 43

3.1. Introdução 43

3.2. Descrição do CCCEE 44

3.2.1. Utilizadores do Centro 44

3.2.2. Rede 46

3.2.3. Servidores e Serviços 47

3.2.4. Recursos de *Hardware* e *Software* 48

3.3. Análise à Gestão das TI do CCCEE 49
3.3.1. Especificação de Requisitos 51
3.4. Conclusão 52
4. **Análise e Implementação de uma Solução de Gestão** 53
4.1. Introdução 53
4.2. Escolha das Ferramentas 54
4.3. Arquitectura da Solução 58
4.3.1. Gestão e Monitorização da Rede 61
4.3.2. Gestão de Inventário 70
4.4. Conclusão 73
5. **Testes e Resultados** 75
5.1. Introdução 75
5.2. Conclusão 85
6. **Conclusões** 87
6.1. Conclusões 87
6.2. Trabalhos Futuros 88
Referências 91
Anexos 95
Anexo A. Fluxo de Processos da Gestão de Eventos, pelo ITILv3 [25] 96
Anexo B. Fluxo de Processos da Gestão de Incidentes, pelo ITILv3 [25] 97
Anexo C. Fluxo de Processos da Gestão de Problemas, pelo ITILv3 [25] 98
Anexo D. Habilitação do SNMP, sob o SO Windows 99
Anexo E. Habilitação do SNMP, sob o SO Linux 100
Anexo F. Configuração do agente Zabbix, sob o SO Windows 101
Anexo G. Configuração do agente Zabbix, sob o SO Linux 102

Lista de Figuras

Figura 1 - Modelo Gestor-Agente [11] 25
Figura 2 - Relação Rede TMN e a Rede de Telecomunicações [11] 27
Figura 3 - Operações de Mensagens do SNMP 29
Figura 4 - Modelo do ciclo de vida de um serviço pelo ITIL v3 [22] 31
Figura 5 – Tipos de gráficos disponibilizados pelo Cacti [38] 36
Figura 6 - Arquitectura do Cacti [40] 37
Figura 7 - Arquitectura do Icinga [45] 38
Figura 8 - Arquitectura do Zabbix [48] 39
Figura 9 - Arquitectura do OCS Inventory NG [52] 40
Figura 10 - Esquema geral da rede do CCCEE 46
Figura 11 – Ferramentas e áreas funcionais de gestão de redes abrangidas 59
Figura 12 - Arquitectura Geral da Solução na Rede do CCCEE 60
Figura 13 - Níveis de gravidade de um problema 67
Figura 14 - Arquitectura do Sistema de Gestão de Alertas 68
Figura 15 – Mapa da Rede 70
Figura 16 - Gráfico da Utilização do CPU no Servidor Apus (11M 10d) (a) 76
Figura 17 - Gráfico da Utilização do CPU no Servidor Apus (16d) (b) 76
Figura 18 - Gráfico da Utilização da Memória do Servidor Apus (11d) 77
Figura 19 - Disponibilidade da página do Moodle 77
Figura 20 – Vista do estado do sistema de ficheiros do servidor Orion (1h) 78
Figura 21 – Vista do estado dos servidores (14d) 78
Figura 22 - Gráfico da Disponibilidade do Servidor ceesoftkeys (20d 3h 19m) 79
Figura 23 – Estado do Sistema de ficheiros do Servidor Orion (1d) 79
Figura 24 - Gráfico das Operações MySQL no Servidor do Zabbix (11M 13d) 80
Figura 25 - Processo de recolha de dados do Zabbix (11M 13d) 80
Figura 26 - Gráfico da utilização do CPU no Servidor Orion (1d) 81
Figura 27 - Informação do *software* instalado num computador, recolhidos pelo OCS Inventory 82
Figura 28 - Resultados da pesquisa de inventário na aplicação OCS Inventory 82

Lista de Tabelas

Tabela 1 - Subfuncionalidades do Modelo FCAPS (baseado em [12]) 23
Tabela 2 - Dados obtidos de um computador pelo Agente OCS 41
Tabela 3 - Servidores WEB utilizados no CCCEE 47
Tabela 4 - Serviços Disponibilizados pelo CCCEE 48
Tabela 5 - Comparação de funcionalidades das Ferramentas (baseado em [32]) 54
Tabela 6 - Grupos de máquinas 60
Tabela 7 - Dados monitorizados nos servidores *Windows* e *Linux* 63
Tabela 8 - Dados monitorizados num *Hypervisor* 64
Tabela 9 - Dados Monitorizados no MySQL 65
Tabela 10 - Dados monitorizados numa impressora 65
Tabela 11 – Proposta de organização das tarefas de gestão e monitorização 68
Tabela 12 - Dados obtidos de uma impressora registada na aplicação OCS, via SNMP 72
Tabela 13 - Exemplos de grupos configurados na aplicação OCS 73

Acrónimos

A3ES	**A**gência de **A**valiação e **A**creditação do **E**nsino **S**uperior
API	***A**pplication **P**rogram **I**nterface*
ASN.1	***A**bstract **S**yntax **N**otation **O**ne*
CCCEE	**C**entro de **C**ompetência de **C**iências **E**xactas e da **E**ngenharia
CCM	**C**entro de **C**iências **M**atemáticas
CEE	**C**iências **E**xactas e da **E**ngenharia
CPU	***C**entral **P**rocessing **U**nit*
DES	***D**ata **E**ncryption **S**tandard*
DHCP	***D**ynamic **H**ost **C**onfiguration **P**rotocol*
DNS	***D**omain **N**ame **S**ystem*
FAX	***Facs**imile*
FCAPS	***F**ault **C**onfiguration **A**ccounting **P**erformance **S**ecurity*
FTP	***F**ile **T**ransfer **P**rotocol*
GLPI	***G**estionnaire **L**ibre de **P**arc **I**nformatique*
HP	***H**ewlett-**P**ackard*
HTTP	***H**yper**T**ext **T**ransfer **P**rotocol*
HTTPS	***H**yper**T**ext **T**ransfer **P**rotocol **S**ecure*
ICMP	***I**nternet **C**ontrol **M**essage **P**rotocol*
IMAP	***I**nternet **M**essage **A**ccess **P**rotocol*
IP	***I**nternet **P**rotocol*
IPMI	***I**ntelligent **P**latform **M**anagement **I**nterface*
IPv	***I**nternet **P**rotocol **v**ersion*
ISO	***I**nternational **O**rganization for **S**tandardization*
ITIL	***I**nformation **T**echnology **I**nfrastructure **L**ibrary*
ITSM	***I**nformation **T**echnology **S**ervice **M**anagement*
ITU	***I**nternational **T**elecommunication **U**nion*
ITU-T	***ITU** –**T**elecommunication Sector*
LDAP	***L**ightweight **D**irectory **A**ccess **P**rotocol*
MAC	***M**edia **A**ccess **C**ontrol*
MB	***M**ega**b**yte*
MD5	***M**essage **D**igest no. **5***
MHz	***M**ega**h**ert**z***
MIB	***M**anagement **I**nformation **B**ase*
OCS	***OCS** Inventory NG*
OGC	***O**ffice of **G**overnment **C**ommerce*
OID	***O**bject **Id**entifier*
OSI	***O**pen **S**ystem **I**nterconnection*
OTRS	***O**pen-source **T**ickets **R**equest **S**ystem*
PDU	***P**rotocol **D**ata **U**nits*
POP	***P**ost **O**ffice **P**rotocol*
qps	***Q**ueries **p**er **S**econd*
RFC	***R**equest **f**or **C**omments*
RRD	***R**ound **R**obin **D**atabase*
SCI	**S**ector de **C**omunicações e **I**nformática
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*
TCP	***T**ransmission **C**ontrol **P**rotocol*
TI	**T**ecnologias de **I**nformação
TMN	***T**elecommunication **M**anagement **N**etwork*
UDP	***U**ser **D**atagram **P**rotocol*
UI	***U**ser **I**nterface*
UMa	**U**niversidade da **Ma**deira
UPS	***U**ninterruptible **P**ower **S**upply*
USB	***U**niversal **S**erial **B**us*
Uuid	***U**niversally **U**nique **Id**entifier*
VLAN	***V**irtual **L**ocal **A**rea **N**etwork*
VM	***V**irtual **M**achine*
XML	*e**X**tensible **M**arkup **L**anguage*
XMPP	***E**xtensible **M**essaging and **P**resence **P**rotocol*

1. Introdução

1.1. Contextualização

A tarefa de gerir uma rede obriga a que exista um controlo de qualquer objecto passível de ser monitorizado, dentro de uma estrutura de recursos lógicos e físicos. De facto, é quase (se não mesmo) impossível mencionar a área de gestão de sistemas e redes sem tocar no campo da monitorização. Enquanto este último campo tem como foco principal a detecção, documentação e notificação de situações anómalas aos responsáveis, a área de gestão centra-se na gestão desses mesmos acontecimentos de modo a corrigi-los e a prevenir a sua ocorrência.

As funções de supervisionamento de uma rede numa organização são, em muitas situações, executadas por pessoas sem experiência em administração de redes, que se deparam continuamente com o desafio de lidar com um vasto leque de equipamentos baseados em tecnologias e fabricantes distintos, obrigando-os a adquirir conhecimentos de áreas de diferentes domínios.

Por outro lado, a interacção entre os vários sistemas heterogéneos de uma rede é estabelecida com base num conjunto de regras que originaram as diversas arquitecturas de redes actuais. Estas últimas especificam quais as funções que uma rede deve realizar e como as executar. O controlo da comunicação, transporte de dados e troca de informação entre sistemas, possibilitam a gestão dos recursos e a coordenação das actividades de uma rede. Através do conhecimento destes mecanismos, conseguiram-se desenvolver soluções que disponibilizam informações sobre o estado geral de uma rede.

Garantir o constante bom funcionamento dos equipamentos e sistemas de uma rede exige, não só, o cuidado nas tarefas de configuração, monitorização e gestão, mas também a capacidade de intervir e desencadear acções correctivas, de forma a manter a disponibilidade dos serviços mesmo nas situações em que surgem falhas ou anomalias inesperadas. Sem um controlo e uma prevenção adequados, o comportamento e desempenho de uma rede pode se degradar e conduzir à anormal operacionalidade dos sistemas e serviços fornecidos aos utilizadores.

Actualmente existem no mercado diversas ferramentas comerciais e/ou de domínio público, que têm por objectivo auxiliar os administradores nas tarefas de gestão e monitorização de sistemas e redes informáticos. Estas ferramentas trabalham continuamente na tentativa de aperfeiçoar as funcionalidades disponibilizadas, tanto a nível de qualidade como de quantidade.

A avaliação e tratamento dos problemas de gestão podem ser aplicados de diversas maneiras como, por exemplo, através de uma visão isolada do problema, i.e., utilizar uma ferramenta diferente para cada tipo de problema, como também por uma visão integrada que

actua sobre uma infra-estrutura como um todo, ou seja, utilizar uma única ferramenta para actuar sobre os vários tipos de problemas. Esta última aproximação exige que os sistemas de gestão de rede sejam compatíveis com os ambientes heterogéneos com os quais os administradores se deparam nas redes informáticas actuais.

Tal investimento, por parte de uma organização, numa solução de apoio, poderá ser justificado, não só pelo *feedback* obtido através dos utilizadores, que vêem assim a possibilidade de usufruir de uma rede com maior fiabilidade nos serviços que disponibiliza, como também para que as próprias organizações se tornem menos dependentes do auxílio de técnicos especializados nas tarefas de gestão. Por outro lado, permite ainda que o gestor de redes perca menos tempo na detecção e correcção dos problemas identificados, podendo dessa forma investir esse tempo na realização de outras tarefas.

Assim, a carga de trabalho efectuada pelos responsáveis pela gestão das tecnologias de informação (TI) de uma organização, que opte por implementar uma solução de apoio, passa por um processo simples de monitorização regular e de pequenas configurações, deixando o "trabalho pesado" para as ferramentas direccionadas para a gestão e monitorização da rede.

1.2. Problema

As dificuldades na área da gestão das tecnologias de informação, dentro de uma organização, crescem à medida que a complexidade, heterogeneidade e dimensão da rede aumentam, uma vez que as necessidades em termos de resposta, controlo e monitorização dos serviços fornecidos aos utilizadores exigem, consequentemente, uma maior atenção e qualidade.

A infra-estrutura informática que se encontra em funcionamento num dos departamentos da Universidade da Madeira, denominado por Centro de Competências de Ciências Exactas e da Engenharia (CCCEE), não está abrangida por um sistema de monitorização que forneça aos gestores as ferramentas e os mecanismos necessários para conseguirem agir de forma preventiva e correctiva sobre os problemas de funcionamento e disponibilidade dos serviços que o CCCEE fornece aos utilizadores.

Nas instalações do CCCEE existem ainda vários tipos de equipamentos e sistemas desactualizados assim como alguns serviços descontinuados, não existindo também um registo actualizado de todos os recursos de *hardware* e *software* do campus informático do CCCEE.

A falta de recursos humanos no CCCEE condiciona também o tempo e a qualidade da resposta que os gestores de rede conseguem fornecer aos pedidos de ajuda dos vários utilizadores, e aos problemas que estes últimos detectam.

Por conseguinte, a necessidade de implementar uma solução que possibilite monitorizar e gerir a rede informática faz-se sentir quer pelos próprios gestores do CCCEE como também por parte dos utilizadores que pretendem usufruir dos serviços fornecidos com qualidade.

1.3. Objectivos da Tese

Quanto maior for o número de sistemas numa organização, maior será o volume de dados a gerir, e mais facilmente a situação pode ficar descontrolada caso a própria infra-estrutura informática não se encontre abrangida tanto por um sistema de gestão e monitorização de rede e sistemas, como também por um sistema de gestão de inventário, que consigam responder às necessidades existentes.

Nas instalações do CCCEE não existem métodos nem políticas de gestão que permitam acompanhar e visualizar o estado do funcionamento e desempenho dos serviços e da rede informática. Assim sendo, para colmatar a ausência de uma solução de monitorização e gestão eficiente de toda a rede e sistemas existentes na rede do CCCEE, pretende-se com o presente projecto o desenvolvimento de um sistema integrado que permita a gestão e monitorização contínua e eficiente dos serviços disponibilizados aos vários utilizadores do CCCEE.

Concretamente, os objectivos a atingir podem ser enumerados da seguinte forma:

1. Permitir uma gestão preventiva da infra-estrutura informática do CCCEE, de forma a prevenir ou evitar que uma situação fora do comportamento normal possa desencadear problemas;

2. Possibilitar uma gestão correctiva, agindo rapidamente sobre os problemas detectados e optimizando o tempo da sua resolução;

3. Melhorar a informação de quais os recursos (*hardware* e *software*) que existem nas instalações do CCCEE;

1.4. Organização da Tese

O presente documento encontra-se estruturado num total de seis capítulos - incluindo o capítulo actual - organizados da seguinte forma:

Capítulo 2: Estado da Arte – são abordados, de forma resumida, os conceitos das principais arquitecturas e os modelos de gestão de redes, sendo ainda identificadas e descritas algumas soluções da área de gestão de redes e sistemas.

Capítulo 3: Gestão de Sistemas e Serviços do CCCEE – refere-se à descrição das características gerais do Centro de Competências de Ciências Exactas e da Engenharia, onde é enquadrado ainda o principal objectivo deste projecto.

Capítulo 4: Análise e Implementação de uma Solução de Gestão – descreve todo o processo de implementação e configuração das soluções aplicadas ao cenário da rede do CCCEE, assim como a abordagem realizada ao problema de gestão existente.

Capítulo 5**:** Testes e Resultados – apresenta e analisa alguns dos resultados obtidos após a implementação das soluções no ambiente real do CCCEE.

Capítulo 6**:** Conclusões – é realizada uma retrospectiva geral do projecto efectuado, identificando-se algumas direcções a seguir, num trabalho futuro, que poderão permitir estender o trabalho até então executado.

Por fim, encontram-se as Referências e os Anexos. O **Anexo A** apresenta o Fluxo de Processos da Gestão de Eventos, pelo ITILv3, o **Anexo B** apresenta o Fluxo de Processos da Gestão de Incidentes, pelo ITILv3, o **Anexo C** apresenta o Fluxo de Processos da Gestão de Problemas, pelo ITILv3, o **Anexo D** apresenta a Habilitação do SNMP, sob o SO Windows, o **Anexo E** apresenta a Habilitação do SNMP, sob o SO Linux, o **Anexo F** apresenta a Configuração do agente Zabbix, sob o SO Windows e o **Anexo G** apresenta a Configuração do agente Zabbix, sob o SO Linux.

2. Estado da Arte

2.1. Introdução

O capítulo Estado da Arte está dividido em três partes. Inicia-se com uma abordagem ao tema da gestão e monitorização das redes, apresentando o Modelo FCAPS (*Fault*, *Configuration*, *Accounting*, *Performance* e *Security*) e as arquitecturas OSI e TMN, assim como o protocolo SNMP presente na arquitectura de gestão de redes TCP/IP. Com base nestas arquitecturas, pretende-se dar a conhecer ao leitor uma base acerca dos mecanismos existentes que possibilitam a comunicação e a troca de informação entre os vários sistemas de uma rede.

As tecnologias de informação (TI) têm vindo a desempenhar um papel importante nas organizações actuais; porém, o sucesso de uma empresa poderá estar ligado, até certo ponto, à forma em como é aplicada a gestão dessas mesmas TI. É com esta linha de raciocínio que se segue com uma descrição do Modelo *Information Technology Infrastructure Library* (ITIL), considerado um dos modelos de referência que disponibiliza uma fonte de estratégias para uma gestão activa e eficiente das tecnologias de informação existentes numa organização.

Os sistemas de gestão e monitorização de rede são, nos dias actuais, um dos elementos mais indispensáveis para que uma rede de computadores funcione com sucesso. A manutenção e configuração de dispositivos de rede, serviços e aplicações, bem como a monitorização contínua do funcionamento e estado de todos estes sistemas de uma rede informática, são os pontos essenciais de um sistema de gestão de uma rede. Desta forma, termina-se o capítulo abordando o tópico das ferramentas de gestão de redes, onde são apresentadas as diferentes abordagens às ferramentas, assim como realizada uma breve descrição das principais características e funcionalidades de algumas ferramentas direcionadas para a área de gestão de redes e sistemas.

2.2. Gestão e Monitorização de Redes

A gestão de redes descreve a metodologia utilizada para gerir e manter a rede operacional, assegurando que os serviços de informação disponibilizados respondem às exigências dos utilizadores. Manter a rede operacional exige conhecimentos técnicos por parte dos administradores das redes informáticas nas áreas de comunicação, sistemas operativos, redes de computadores, comunicação de dados, administração de redes, entre outras. Conseguir complementar, a gestão e monitorização das componentes práticas e teóricas de todas essas áreas, tem sido um desafio constante para várias entidades que têm trabalhado no desenvolvimento de modelos e/ou arquitecturas que ajudem a garantir o complemento dessas componentes.

O modelo FCAPS (*Fault*, *Configuration*, *Accounting*, *Performance* e *Security*) é um dos principais contributos para a gestão de infra-estruturas informáticas, decompondo e categorizando os objectivos das tarefas de gestão de redes. Foi desenvolvido pela ITU - *Telecommunication Sector* (ITU-T) e pela *International Organization for Standardization* (ISO), servindo de referência para vários outros modelos.

Os modelos e padrões das arquitecturas *Open System Interconnection* (OSI) [1], *Telecommunication Management Network* (TMN) [2] e arquitectura de gestão de redes TCP/IP (onde se inclui o protocolo SNMP), representam as abordagens tradicionais por se tratar de normas maduras, aceites e aplicadas por muitas entidades da área das redes.

Os princípios para a arquitectura gestão de redes OSI da organização ISO são definidos em dois documentos: o OSI *Management Framework* [3] e o OSI *System Management* [4]. Ambos surgem após o OSI *Basic Reference Model* [5] onde foi enquadrada a gestão da rede no modelo de camadas e, adicionalmente, algumas definições iniciais para a gestão de redes [6].

As definições arquitecturais do modelo de comunicação TMN/ITU-T e os seus princípios encontram-se definidos no documento *M.3010 Principles for* TMN [2]. As funções associadas aos serviços de gestão são apresentadas nos documentos da série *M.3200* TMN *Management Services Introduction* [7]. Os demais documentos da série M descrevem a metodologia e terminologias do modelo em questão.

Por sua vez, os padrões enquadrados na gestão da internet, ou de redes TCPI/IP, encontram-se publicados numa série de documentos denominados por *Request for Comments* (RFC) [8]. Estes RFCs são uma série progressiva de relatórios, propostas e padrões de protocolos que descrevem os trabalhos internos do padrão TCP/IP e da Internet [9].

Na secção 2.2.1 descreve-se o modelo FCAPS que identifica as cinco funcionalidades da área de gestão de redes. A secção 2.2.2 apresenta as principais abordagens à gestão de redes, enquadradas nas normas apresentadas anteriormente, a arquitectura de gestão OSI e TMN. Por fim, na secção 2.2.3 é descrito o protocolo SNMP como principal método de monitorização.

2.2.1. Modelo FCAPS

Conceptualmente, a gestão de redes encontra-se divida em cinco áreas funcionais, que podem ou não estar todas incluídas num mesmo sistema de gestão. Tradicionalmente, essas áreas são designadas pela sigla FCAPS, do acrónimo *Fault*, *Configuration*, *Accounting*, *Performance* e *Security*, que podem ser traduzidos para português como: Falhas, Configuração, Contabilização, Desempenho e Segurança, estando descritos mais à frente.

A ideia base do modelo FCAPS [10] [11] [12] é categorizar a grande quantidade de informações tratadas por um sistema de gestão e monitorização, nas suas respectivas áreas funcionais, como apresentado na Tabela 1.

Tabela 1 - Subfuncionalidades do Modelo FCAPS (baseado em [12])

FAULT	*CONFIGURATION*	*ACCOUNTING*	*PERFORMANCE*	SECURITY
Detecção de Falhas	Inicialização de Recursos	Serviço de Rastreio / Utilização de Recursos	Utilização & Taxas de Erros	Acesso Selectivo de Recursos
Correcção de Falhas	Provisionamento da Rede	Custo dos Serviços	Nível de Desempenho Constante	Activação de Funções da Rede
Isolamento de Falhas	Auto Descoberta	Limite Contabilístico	Recolha de Dados de Desempenho	Acesso a *Logs*
Recuperação da Rede	*Backup* e Restauro	Relação de Custos para Múltiplos Recursos	Geração de Relatórios de Desempenho	Alarmes de Segurança / Relatório de Eventos
Tratamento de Alertas	Desactivação de Recursos	Estabelecimento de Quotas de Utilização	Análise de Dados de Desempenho	Privacidade de Dados
Filtragem de Alertas	Gestão de Alterações	Audições	Relatório de Problemas	Verificação de Permissões de Acesso
Geração de Alertas	Pré-provisionamento	Relatório de Fraudes	Capacidade de Planeamento	Resolução de Quebras da Segurança
Correlação Clara	Inventário/Gestão de Activos	Suporte de vários Métodos Contabilísticos	Dados de Desempenho / Recolha de Estatísticas	Auditoria de Segurança
Testes de Diagnóstico	Cópia de Configurações		Manutenção e Análise de Históricos	Actualização de Informação Relacionada com Segurança
Relatórios de Erros	Configurações Remotas			
Estatísticas de Erros	Inicialização do Trabalho			
	Rastreio e Execução			
	Actualizações Automáticas			

As principais actividades da gestão de **falhas** (F - *Fault*) incluem a detecção, registo, diagnóstico e resposta a condições de problemas na rede. A detecção é feita com base em acções de monitorização de eventos - como a ocorrência de alarmes gerados por dispositivos de rede – sendo, por regra, criados registos desse mesmo erro para uma possível análise futura.

A detecção e o diagnóstico de falhas conduzem frequentemente à geração de notificações que, posteriormente, levam o próprio sistema e/ou um gestor de rede a desencadear acções para a sua resolução. A resolução poderá exigir, em situações mais complexas, a intervenção de equipas de campo ou apenas uma simples alteração da configuração de alguns elementos da rede. Por outras palavras, a gestão de falhas consiste basicamente em monitorizar a rede para garantir que a mesma se encontra em bom estado e possibilitar uma resposta pronta, quando tal situação não se verificar.

A tarefa de configuração de elementos da rede, referida no parágrafo anterior, já se enquadra na área da gestão de **configuração** (C - *Configuration*). Esta, reúne um conjunto de funções que permite a um administrador de redes obter, monitorizar e alterar informações de configuração do sistema, possibilitando o controlo dos dispositivos de *hardware* e *software* que integram a rede.

As tarefas de **contabilização** (A – *Accounting*) permitem registar e controlar a utilização dos recursos/serviços e dispositivos da rede por parte dos utilizadores, entre outros. Trata-se de um elemento essencial para o suporte de actividades das áreas de gestão anteriormente mencionadas, contendo funções de recolha de informação de modo a quantificar, medir, reportar, analisar e controlar o desempenho dos dispositivos da rede. A gestão da contabilização apresenta um papel importante nas situações em que as redes são privadas, possibilitando a definição de diferentes modelos de negócio, ou seja, conseguir ajustar a taxação à utilização da rede por parte dos clientes/utilizadores. Contudo, mesmo em redes não comerciais, a contabilização da utilização dos recursos de rede permite determinar padrões que possibilitarão descobrir e conhecer com detalhe o consumo de alguns ou de todos os recursos, podendo auxiliar, por exemplo, no apoio à tomada de decisões de evolução da rede. Um aspecto a salientar é a importância de garantir que os dados de contabilização recolhidos são fidedignos. Caso contrário, isso poderá acarretar tomadas de decisões erradas levando ao fornecimento de serviços quase gratuitamente, entre outras situações.

A informação relativa ao **desempenho** (P - *Performance*) - de elementos físicos ou lógicos da rede – poderá ser utilizada para caraterizar o comportamento da rede de forma a prever o seu desempenho futuro ou a apoiar as decisões de planeamento, permitindo uma gestão pró-activa. A gestão do desempenho é importante para assegurar a qualidade dos serviços necessários às aplicações, como ainda para garantir que essa qualidade é atingida com poucos custos. Esta área funcional pode ser vista como um subconjunto da gestão de falhas, uma vez que as duas envolvem a identificação e eliminação de problemas que levam à diminuição da produtividade na rede, divergindo apenas na forma em como essa redução de produtividade afecta a organização.

Este planeamento também poderá abranger o factor de **segurança** (S - *Security*) que inclui todas as actividades relacionadas com o controlo de acesso aos recursos, como a criação de grupos e respectivos privilégios, e com a configuração e monitorização de sistemas de segurança, tudo de acordo com a política da organização. Há que ter em conta não só a gestão da segurança, mas também a segurança da gestão. Isto significa que a própria gestão

(operações de gestão) tem de ser segura, i.e., o acesso às operações de gestão e monitorização deve ser restrito a utilizadores autorizados.

É de referir que estas áreas funcionais não são estanques, nomeadamente, há várias funções da gestão que dependem da configuração. Por exemplo, uma falha não pode ser bem diagnosticada sem um conhecimento preciso das configurações actuais da rede. Por outro lado, não se devem fazer muitas alterações nas configurações ao mesmo tempo, pois se alguma coisa correr mal, é mais difícil saber o que causou o problema, fazendo da gestão de falhas o novo objectivo. Para além da sua importância para o planeamento da rede, a gestão de desempenho é essencial no suporte de actividades de configuração e gestão de falhas.

2.2.2. Arquitecturas de Gestão OSI e TMN

A comunicação entre sistemas só é atingível dentro de um contexto de regras que estabelecem as interacções entre os equipamentos e/ou módulos de programas. Normalmente, o conjunto formado por essas regras é designado por arquitectura, sendo que estas regras definem e descrevem vários conceitos aplicáveis à comunicação de sistemas. Independentemente de qual (ou quais) os modelos de gestão de redes que sejam implementados, o seu principal objectivo é sempre o mesmo: garantir o bom funcionamento da rede, divergindo apenas na abordagem com que esse objectivo é alcançado.

Uma condição essencial para se ter uma arquitectura de gestão, é a mesma consistir em quatro submodelos genéricos [13]: Modelo de Informação, Modelo Organizacional, Modelo de Comunicação e Modelo Funcional – descritos de seguida –, os quais têm, normalmente, por base, uma arquitectura do tipo gestor-agente como apresentado na Figura 1.

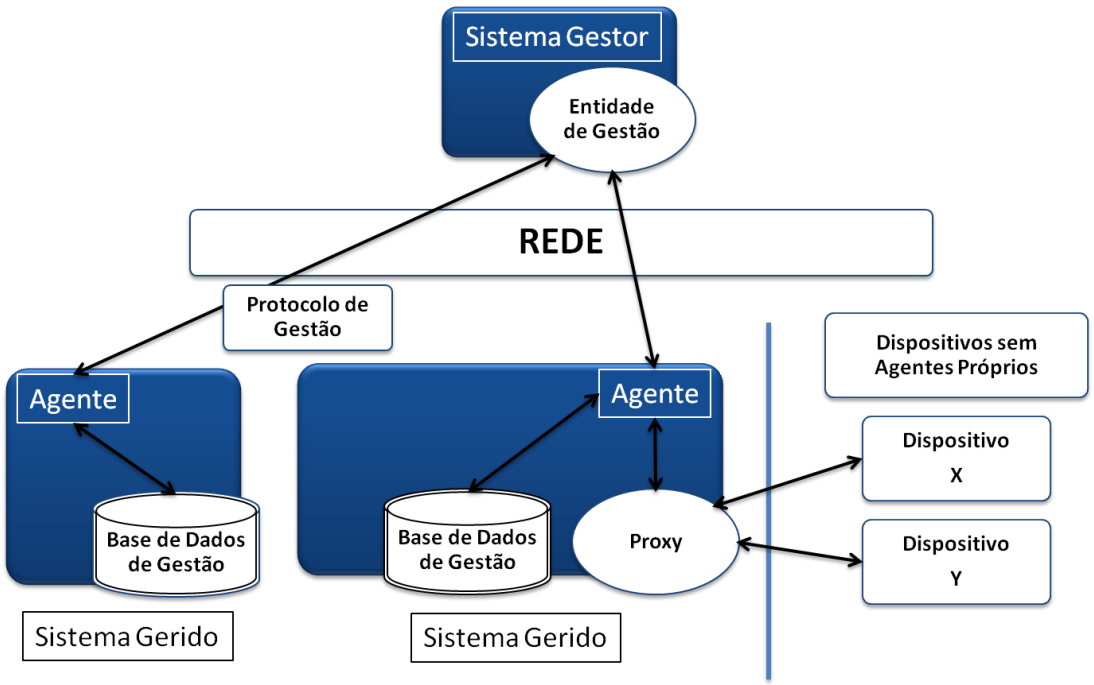


Figura 1 - Modelo Gestor-Agente [11]

O 'Modelo de Informação' especifica uma sintaxe e semântica comum aos objectos geridos de forma a modelar os parâmetros relevantes para a gestão. A definição da sintaxe e da semântica da informação de gestão que define os objectos é realizada pela *Structure of managements Information* (SMI) e é armazenada na *Management Information Base* (MIB). A utilização da SMI garante que não existe ambiguidades na linguagem de informação, através da utilização da ASN.1 (*Abstract Syntax Notation One*).

O 'Modelo Organizacional' define quais as responsabilidades e os papéis (gestor e/ou agente) a atribuir aos diferentes objectos existentes no sistema, dependendo do tipo de topologia implementada [13]: na topologia multiponto, cada recurso gerido é associado a um determinado grupo (domínio), sendo atribuído a cada domínio um gestor. Na abordagem centralizada, existe apenas um sistema de gestão central que controla e é responsável pelas tarefas de gestão. Por fim, a aproximação multi-centralizada e hierárquica permitem coordenar, dependendo do esquema de cooperação, os gestores de uma aproximação multiponto.

Os mecanismos para a troca de informação de gestão entre o gestor e o agente, são definidos pelo 'Modelo de Comunicação', que especifica os protocolos e serviços para a realização nessa tarefa.

O último, o 'Modelo Funcional', identifica as áreas funcionais (*Fault*, *Configuration*, *Accounting*, *Performance*, *Security*) e define os serviços e funções de gestão genéricos esperados para cada área, assim como os objectos importantes a gerir.

As principais arquitecturas de gestão de redes, a OSI e a TMN, incluem também quatro submodelos específicos para cada uma das arquitecturas [11] [14], embora se baseiem nos conceitos genéricos dos submodelos do modelo gestor-agente aqui descritos.

Na arquitectura de gestão OSI, o modelo de Informação define uma aproximação do tipo orientada a objectos (*object-oriented*), incluindo ainda o princípio de herança e o alomorfismo (*allomorphism*) [13]. O princípio de herança define que um objecto pode pertencer a uma subclasse ou a várias superclasses, herdando as respectivas propriedades, isto significa que quanto mais refinada é uma classe mais a informação de um objecto se torna específica e vice-versa (ex: dispositivo, impressora, impressora a laser, HP *LaserJet*). O princípio de alomorfismo significa que um recurso pode ser visto como um objecto gerido ou como uma instanciação de diferentes classes de objectos na hierarquia de herança, permitindo assim que os recursos de um objecto sejam divididos em grupos que, no âmbito da gestão, devem ser tratados de modo semelhante. Assim, é possível simplificar as tarefas de gestão, gerindo por exemplo, uma impressora a laser como uma entidade da classe "*laser print*" ou como uma entidade da classe "*output device*", gerindo um grupo de dispositivos da mesma classe da mesma forma, em vez de cada dispositivo por si.

O segundo modelo – Organizacional – define os dois papéis mais importantes para as entidades de gestão: o papel de gestor (*Manager*) e de agente (*Management Agent)* [14]. O gestor fica responsável pela execução das acções de gestão enquanto o agente recebe os pedidos e envia as respostas e notificações ao mesmo. A interacção entre as duas entidades ocorre através da utilização dos protocolos de gestão. Os sistemas OSI podem, em certas operações, assumir os dois papéis alternando-os dinamicamente; adicionalmente, um

dispositivo de rede também poderá conter vários agentes de gestão. Uma pequena descrição de ambos os papéis é apresentada na secção 2.2.3.

O modelo de comunicação OSI integra três mecanismos que possibilitam a troca de informação de gestão entre o agente e o gestor e que cobrem três áreas distintas da gestão: gestão de sistemas, gestão de camadas e gestão de protocolos, contudo não define como as mesmas interagem entre si [11].

Por sua vez, o Modelo Funcional divide as funcionalidades da gestão em cinco áreas distintas [12], denominadas por FCAPS, como apresentado na secção 2.2.1.

Da mesma forma que a arquitectura OSI, a arquitectura TMN, representada na Figura 2, também se define através dos modelos enumerados anteriormente, dando especial atenção ao Modelo Organizacional, que toma em consideração o contexto particular das redes públicas, e no Modelo Funcional que identifica cinco blocos funcionais: Funções Sistemas de Operações (*Operations System Functions*), Funções Estações de Trabalho (*Work Station Functions*), Funções Q Adaptador (*Q Adaptor Functions*), Funções Elementos de Rede (*Network Element Functions*) e Funções de Mediação (*Mediation Functions*) [11].

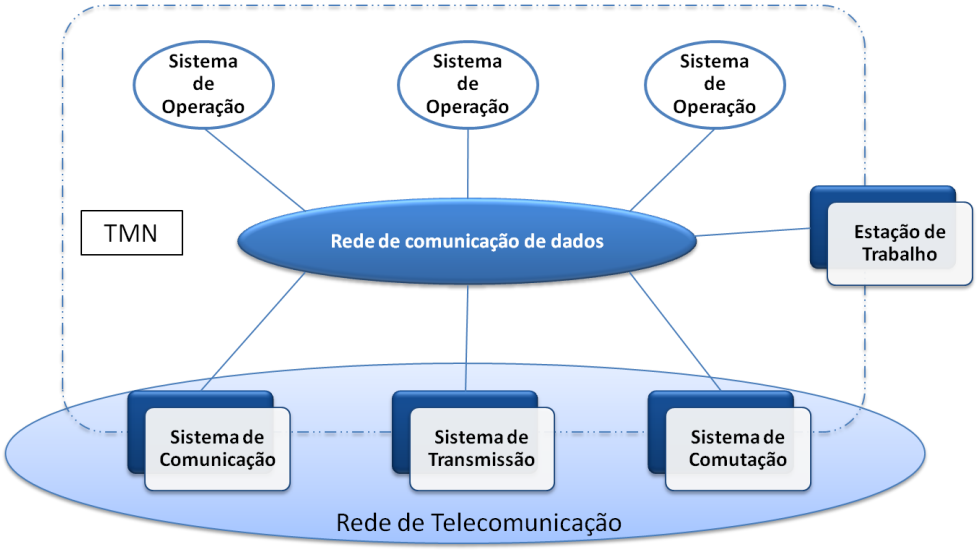


Figura 2 - Relação Rede TMN e a Rede de Telecomunicações [11]

O principal papel da TMN centra-se na área de gestão das redes de telecomunicações, tendo por objectivo proporcionar a gestão homogénea de redes heterogéneas, que compõem actualmente as redes utilizadas pelos operadores de telecomunicações. Ou seja, esta arquitectura possibilita que diferentes equipamentos de diferentes fornecedores sejam geridos através de uma estrutura organizada, que permite interligar diversos tipos de sistemas de administração/gestão, abrangendo todas as áreas funcionais do FCAPS e suportando uma gestão integrada especificamente desenhada para as redes de telecomunicações. Para além disso, nesta arquitectura a gestão das redes de telecomunicações é feita por uma rede de gestão distinta da rede a gerir.

Embora o âmbito de actuação desta arquitectura não se adeque ao género de rede estudada neste projecto, os conceitos nela presentes, assim como nas demais arquitecturas de gestão apresentadas, são de grande utilidade na área da gestão e monitorização de sistemas e redes auxiliando, por exemplo, na compreensão em como as plataformas de gestão actuam sobre os recursos lógicos e físicos existentes na rede.

2.2.3. Arquitectura de Gestão da Internet

Na arquitectura de gestão da internet, ou de redes TCP/IP, é dada maior importância aos modelos de informação e comunicação. O modelo de informação do TCP/IP, faz uso de uma árvore de registo que possibilita a identificação da informação de gestão através de uma árvore de nomeação que permite definir e reconhecer, de forma unívoca, os identificadores de objectos (*Object Identifier*, OID), que são únicos à escala global [15]. O modelo de comunicação assenta na utilização do principal componente de gestão mais utilizado nas redes informáticas, para a troca de informação de gestão entre dispositivos, o protocolo *Simple Network Management Protocol* (SNMP) [16].

Embora o SNMP esteja fortemente ligado ao TCP/IP, este foi desenvolvido pelo organismo de normalização *Internet-Standard Management Framework (ISMF)*. Deste modo, o termo SNMP torna-se um pouco ambíguo, pois pode ser utilizado para se referir ao próprio protocolo de comunicação, como também para se mencionar o conjunto de tecnologias que permitem gerir redes TCP/IP.

Independentemente do contexto em que é introduzido, o papel do SNMP é o de fornecer um mecanismo para gerir e monitorizar dispositivos de *hardware* e *software* que se encontram ligados à rede, independentemente do fabricante. Assim, numa rede monitorizada e gerida pelo SNMP, existem três componentes básicos [10]:

- **Estação de Trabalho ou Gestor** - tipicamente um computador, utilizado para executar um ou mais sistemas de gestão de redes, que contem uma aplicação que possibilita a um administrador - por via de uma interface - recolher informações e controlar os dispositivos de rede.

- **Agentes -** consistem em módulos de *software* que contém um conhecimento local da informação de gestão dos dispositivos onde são implementados, e que traduzem essa informação de modo a ser compatível com o SNMP para responder às consultas (*queries*) por parte da entidade de gestão.

- ***Management Information Base*** (MIB) – trata-se de uma base de dados virtual que reúne e armazena objectos geridos, os quais são basicamente dados de informação de gestão de um dispositivo. Uma MIB é constituída por uma estrutura hierárquica em árvore, em que cada objecto contém um OID, que define a sua localização na árvore, um nome e um tipo (por exemplo “inteiro”).

Nesta arquitectura é definido o conceito de agente *proxy*, que não existe no modelo OSI, e que tem como objectivo permitir a gestão dos recursos de um dispositivo que não comporte ou não utilize um agente ou os mesmos protocolos de comunicação e gestão.

As mensagens - ou PDU (*Protocol Data Units*) – do SNMP trocadas entre gestor-agente são enviadas normalmente em pacotes pelo protocolo de transporte UDP, mas também são permitidas outras alternativas. O modo de operação mais comum do protocolo SNMP, apresentado na Figura 3, designa-se por *polling* e é quando o gestor é o responsável por iniciar a comunicação com o agente, com o objectivo de obter dados relacionados com os dispositivos da rede. Na comunicação inversa, quando o agente pretende notificar o gestor acerca de uma alteração anormal de um determinado objecto, o processo é denominado por *trap* [17].

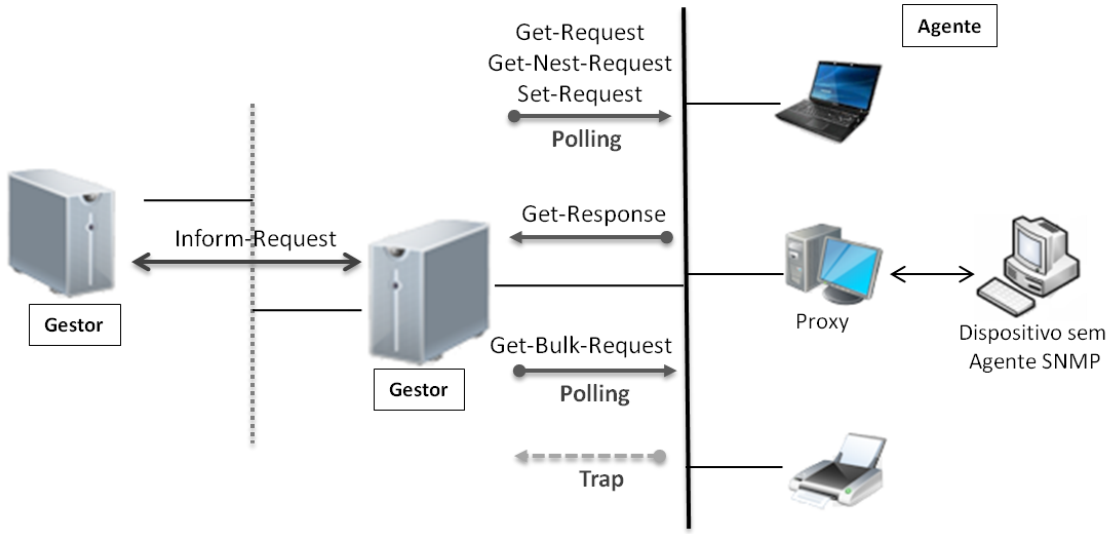


Figura 3 - Operações de Mensagens do SNMP

Na primeira versão do SNMP, as operações suportadas na comunicação do gestor para os agentes incluíam as mensagens: *Get-Request*, *Get-Next-Request* e *Set-Request*, que são respondidas pelos destinatários com uma mensagem do tipo *Get-Response*. As operações *Get-Bulk-Request* e *Inform-Request* foram incluídas na versão seguinte do protocolo com o objectivo de optimizar a transferência de grandes volumes de dados e de possibilitar a comunicação entre gestores, respectivamente.

No SNMP, os mecanismos de segurança aplicados na proteção dos dados transmitidos na comunicação envolvendo as entidades gestor e agente, foram alvo de algumas actualizações nas diferentes versões do protocolo.

Na primeira versão do protocolo SNMP utilizou-se um método simples designado por '*community string*', em que o nome da mesma funcionava como palavra-chave que era partilhada entre a entidade gestor e a entidade agente.

Na versão seguinte deste protocolo (SNMPv2), os métodos de segurança basearam-se nos seguintes mecanismos [13]:

- **Autenticação** – utiliza o algoritmo MD5 (*Message Digest no. 5*) para autenticar a comunicação entre o servidor SNMP e o agente SNMP, verificando a integridade das comunicações;

- **Encriptação** – utiliza o algoritmo DES (*Data Encryption Standard*) para encriptar a informação, e;

- **Procedimento de temporizador** (*time stamp*) – verifica se a sequência das mensagens está ou não em ordem, de modo a evitar duplicação de mensagens.

No entanto, pelos mecanismos de segurança apresentados anteriormente serem mais complexos, não tiveram uma boa aceitação no mercado. Desta forma, surgiu o SNMPv3 que adiciona ao SNMPv2c (**c** de "*community*") novos mecanismos de segurança [18]: autentificação, privacidade, autorização e controlo de acesso (para limitar o que diferentes grupos podem ver e fazer). Tornando, finalmente, o SNMP, um protocolo mais seguro.

O protocolo SNMP tem a capacidade de monitorizar uma rede completa, pois pode ser aplicado não só a dispositivos físicos (*Windows*, *Unix*, impressoras…) como também pode ser aplicado a *softwares* (servidores, base de dados, …). Por esta razão – e apesar do SNMPv3 ainda não ser suportado por vários agentes, pelos seus fortes mecanismos de segurança –, este protocolo encontra-se presente em grande parte das ferramentas actuais enquadradas na área de gestão e monitorização de sistemas e redes.

Na secção 2.3 é apresentado e descrito o Modelo ITIL, direcionado para as organizações que fornecem serviços de TI.

2.3. Modelo ITIL

A evolução das tecnologias de informação (TI) exige, cada vez mais, a necessidade de reconhecer que os serviços de TI são recursos activos importantes dentro de uma organização, levando os gestores a trabalhar ininterruptamente com o desafio de coordenar e desenvolver estratégias de gestão para fornecer serviços de TI de alta qualidade.

O Modelo *ITIL* (*Information Technology Infrastructure Library*) [19] [20] surge, portanto, como um conjunto de regras que descrevem as melhores práticas para a gestão de serviços de tecnologias de informação (*ITSM*), focando-se tanto numa perspectiva de negócio como na perspectiva do cliente. Este modelo permite a certificação de pessoas na área da gestão de TI e possibilita, ainda, a várias organizações, desenvolver uma consciência sobre as suas verdadeiras necessidades em relação aos seus serviços de TI e ao fornecimento desses serviços aos clientes.

Devido às constantes evoluções no mercado e das novas tecnologias, este modelo vem sofrendo frequentes alterações desde a sua criação, entre as quais a que deu origem à versão dois (*ITIL v2*) – já sob o domínio da *OGC* (*Office of Government Commerce*) – e a que deu origem à actual versão três (*ITIL v3*), no ano de 2007 [21].

A arquitectura principal do *ITIL* baseia-se num total de cinco estados (*Service Strategy*, *Service Design*, *Service Transition*, *Service Operation* e *Continual Process Improvement*), que definem as diferentes fases do ciclo de vida de um serviço, apresentado na Figura 4. Antes de detalhar cada um dos cinco estados, é importante explicar o conceito de serviço. Desta forma, o *ITIL* define um serviço como "um meio de entregar valor aos clientes, facilitando os resultados que um cliente quer alcançar sem a posse de custos e riscos específicos" [19].

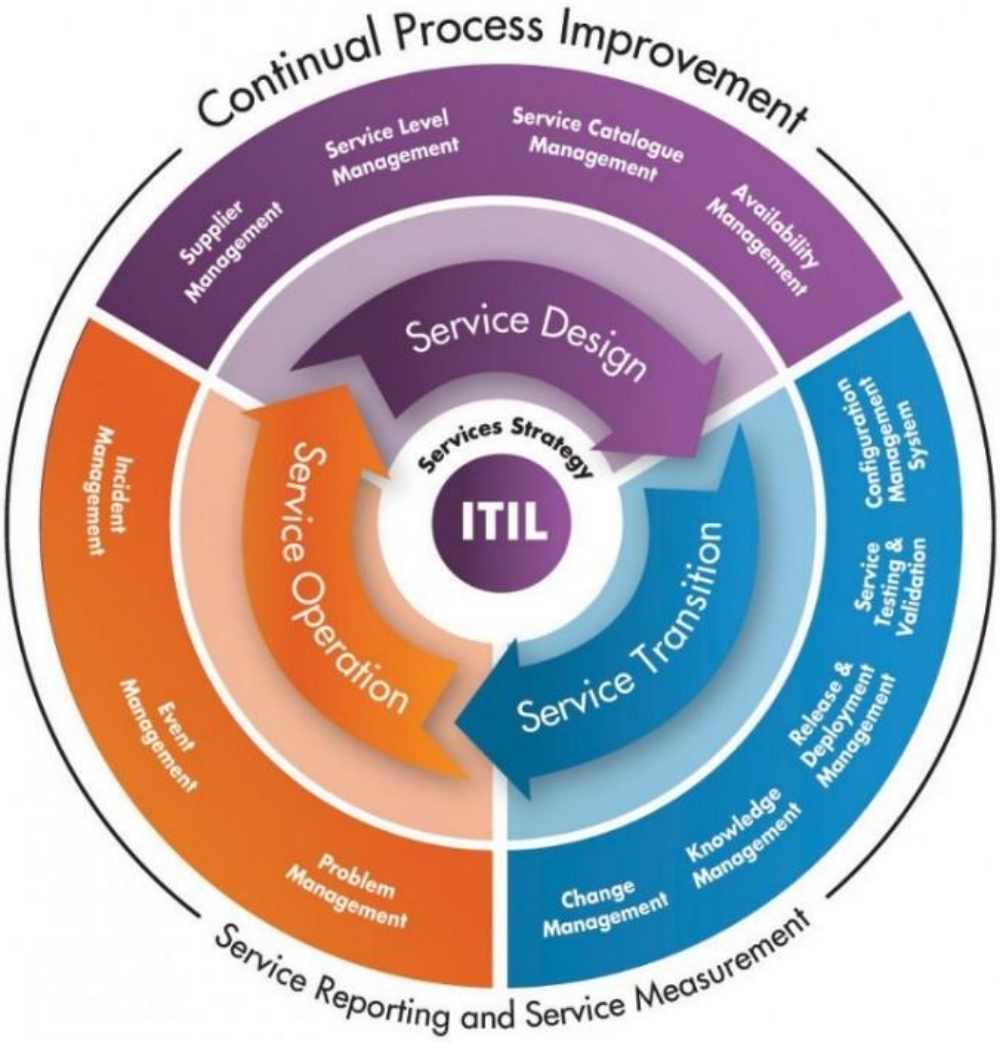


Figura 4 - Modelo do ciclo de vida de um serviço pelo ITIL v3 [22]

Cada um dos cinco estados, descritos de seguida, está publicado em livros que, no seu conjunto, explicam como os serviços devem ser selecionados (*Service Strategy*), desenhados (*Service Design*), introduzidos (*Service Transition*), operados (*Service Operation*) e melhorados (*Continual Process Improvement*) numa organização.

O estado **Estratégia de Serviço** (*Service Strategy*) [23] é o eixo em torno do qual gira o ciclo de vida de um serviço, em que são identificadas as necessidades dos clientes e dos requisitos de TI, e contém três processos chaves:

- Gestão Financeira (*Financial Management*) – foca-se na quantificação do valor dos serviços de TI, bem como na qualificação da previsão operacional;
- Gestão do Portfólio do Serviço (*Service Portfolio Management*) – envolve uma gestão pró-ativa do investimento, em todo o ciclo de vida do serviço;
- Gestão da Procura (*Demand Management)* – tem por objectivo compreender a procura dos clientes e a capacidade de atender a essa procura.

No estado ***Design* de Serviço** (*Service Design)* [24] desenvolve-se o desenho da nova solução, sendo um elemento importante dentro do processo de mudança no negócio da organização, no fornecimento de serviços de TI. Este estado abrange os seguintes processos principais:

- Gestão de Fornecedores (*Supplier Management)* – tem como objectivo garantir que os fornecedores executam as metas acordadas nos contratos, em conformidade com todos os termos e condições;
- Gestão dos Níveis de Serviços (*Service Level Management)* – o seu objectivo é assegurar que o desempenho de todos os serviços operacionais é medido de forma consistente e profissional em toda a organização de TI;
- Gestão do Catálogo de Serviços (*Service Catalog Management)* – fornece uma fonte única de informações sobre todos os serviços, garantindo que a mesma se encontra disponível;
- Gestão da Disponibilidade (*Availability Management)* – envolve todas as questões relacionadas com a gestão da disponibilidade de serviços, componentes e recursos, garantindo que as metas em todas as áreas são alcançadas de acordo com as necessidades de disponibilidade do negócio.

No terceiro estado, **Serviço de Transição** (*Service Transition)* [25], passa-se à construção e implementação do serviço. Este estado integra também processos que não são apenas exclusivos deste estado, tais como: o processo de Testes e Validação de Serviços (*Service Testing and Validation)* e o processo de Gestão de Lançamento e Implementação (*Release and Deployment Management).* Integra, ainda, alguns dos processos mais importantes de todo o ciclo de vida de um serviço, que têm impacto em todos os outros estados, entre os quais:

- Sistema de Gestão de Configuração (*Configuration Management System)* – identifica, controla e conta os serviços activos e itens de configuração, protegendo e garantindo a sua integridade através do ciclo de vida do serviço;
- Gestão do Conhecimento (*Knowledge Management)* – tem como principal meta garantir que a pessoa certa tem o conhecimento certo, na hora certa, para apoiar os serviços exigidos pelo negócio;

- Gestão de Mudança (*Change Management)* – utiliza métodos padrão para um tratamento rápido e eficiente de todas as mudanças, mantendo um registo das alterações para que o risco global do negócio seja optimizado.

É no estado **Operação de Serviço** (*Service Operation)* [26] que os serviços são entregues e que realmente agregam valor ao negócio. É também neste estado que se identifica os "sinais vitais" que são fundamentais para a execução de funções importantes para a organização. Tem como principais processos:

- Gestão de Eventos (*Event Management)* – gera e detecta notificações enquanto verifica e monitoriza o estado dos componentes, mesmo na inexistência de algum evento;
- Gestão de Incidentes (*Incident Management)* – o seu objectivo é restaurar, o mais rápido possível, a normalidade de um serviço e minimizar esse impacto na operação do negócio;
- Gestão de Problemas (*Problem Management)* – inclui o diagnóstico das causas de um problema, determinando e implementando a sua resolução de forma a minimizar que os mesmos se repitam.

O último estado do ciclo, **Melhoria Contínua do Processo** (*Continual Process Improvement)* [27], preocupa-se com a satisfação dos clientes, identificando e implementando os melhores métodos através de uma avaliação e melhoria contínua da qualidade dos serviços. Neste estado, são definidos três processos:

- Processo de Aperfeiçoamento de 7-etapas (*7-Steps Improvement Process)* – abrange os passos necessários para recolher dados significativos, analisar os dados para que sejam identificadas tendências e problemas, apresentar as informações de gestão para o estabelecimento de prioridades e para a implementação de aperfeiçoamentos;
- Medição de Serviços (*Service Measurement)* – apresenta três tipos de métricas: de tecnologia, de processo e de serviço, que uma organização necessita para suportar um aperfeiçoamento contínuo de várias actividades;
- Relatório de Serviços (*Service Reporting)* – preocupa-se com a criação de um relatório, que incida sobre o futuro, mas se concentre também no passado, fornecendo os meios necessários para se "entrar" no mercado, mantendo as experiências positivas e negativas do negócio directamente alinhadas.

De uma forma geral, o Modelo ITIL é desenhado para descrever os processos, actividades, tarefas e listas de verificação a serem desempenhadas pelo administrador na gestão de serviços de tecnologias de informação. Todo este conjunto de acções a desempenhar não são específicas de um único tipo de organização podendo, por isso, ser aplicadas e adaptadas por várias organizações para estabelecerem um nível mínimo de qualidade nos serviços que fornecem.

No Modelo ITILv3 foram também estabelecidas relações de compatibilidade com outros dois modelos de gestão: o modelo ISO/IEC 20000:2011 [28] e o COBIT5 [29]. Trabalhos como [30] e [31] comparam os três modelos de gestão de serviços de TI. Enquanto o ITIL está projectado para certificar pessoas na área de gestão de TI, explicando como trabalhar com as tecnologias de informação, descrevendo quais as tarefas e a ordem pelas quais devem ser realizadas, o modelo ISO/IEC direcciona-se para a certificação da organização que fornece os serviços de TI, disponibilizando para esse objectivo um conjunto de requisitos simples, mas rigorosos, de implementação obrigatória, independentemente da ordem pela qual os requisitos são aplicados. Por sua vez, o padrão COBIT foca-se no controlo dos negócios das organizações que integram ou fornecem serviços de TI.

Na próxima e última secção deste capítulo, serão apresentadas as ferramentas de gestão de redes, onde serão descritas as principais funcionalidades das ferramentas selecionadas.

2.4. Ferramentas de Gestão de Redes

Gerir uma rede de TI trata-se de uma actividade complexa, por mais pequena ou simples que seja a rede. A grande proliferação de sistemas heterogéneos que se encontram conectados à rede poderá ter como consequência directa o incremento da complexidade dessas tarefas de gestão. Por este motivo, a implementação de uma ferramenta que auxilie neste processo, terá que ser adequada à realidade de um determinado ambiente, devendo ser realizada com algum cuidado pois poderá acarretar, em determinadas situações, alguns custos.

Os trabalhos em [10] e [11] fornecem uma análise a um conjunto de critérios que ajudam no processo de comparação e selecção das ferramentas, sendo estes: a funcionalidade, extensibilidade, abertura, segurança, actualização tecnológica, aplicações e custo.

O número de **funcionalidades** de uma ferramenta implicará uma redução da quantidade de trabalho executado manualmente por um administrador de redes. No entanto, quantas mais funcionalidades a ferramenta incorporar, mais longo poderá ser o processo de aprendizagem de utilização da mesma.

O critério da **extensibilidade** assegura que uma plataforma tem a capacidade de se adaptar ao crescimento de uma rede, ganhando este critério maior importância para redes sujeitas a actualizações e incrementações frequentes.

O nível de **abertura** disponibilizada por uma ferramenta é talvez a característica mais relevante, pois define se a ferramenta suportará a interacção com equipamentos de natureza e fabricantes diferentes e ainda a capacidade de integração com outras plataformas.

A **segurança** na área das redes é, pela sua própria natureza, um factor de extrema importância para todas as organizações. Deste modo, as plataformas devem integrar, por exemplo, mecanismos de autenticação que impeçam a sua utilização indevida. Contudo, por norma, as organizações deixam esta responsabilidade a cargo de ferramentas especializadas na área da segurança.

O critério da **actualização tecnológica** implica que, pela constante evolução das TI, as ferramentas de gestão devem ser capazes de suportar as tecnologias mais recentes, actualizando-se quer em termos de modelos de informação como de comunicação.

A possibilidade de adição de **novas aplicações** às funções básicas de uma ferramenta é das características mais "desejáveis" para os administradores, incrementando assim o número de funções e tarefas fornecidas inicialmente pela plataforma.

Dos critérios identificados, o **custo** é o principal determinante no nível de abrangência final da ferramenta selecionada, pois os demais critérios terão de ser adequados em conformidade com este último critério, existindo dois tipos de investimento: monetário (existente, por exemplo, nas ferramentas comerciais) e o custo de aprendizagem/adaptação à ferramenta (mais frequentes nas ferramentas *open source*).

Por outro lado, existem três abordagens distintas para a criação de ferramentas [13]: isolada, coordenada e integrada.

Na abordagem **isolada**, as plataformas são criadas para funcionarem em equipamentos de apenas um vendedor em particular, funcionando cada ferramenta de modo independente para cada problema de gestão e/ou área funcional, através de *interfaces* também independentes. Esta solução não deverá ser implementada em redes complexas e heterogéneas por exigir, por exemplo, elevados custos de operação.

Numa abordagem **coordenada** as ferramentas ainda funcionam de forma independente, não existindo qualquer uniformidade entre os dados. Contudo, as diferentes ferramentas conseguem complementar-se (controladas através de uma *interface* comum), interagindo através da produção de *scripts*, pois o *output* de uma ferramenta poderá ser utilizado como *input* para outra.

Para a abordagem **integrada** devem ser especificados e cumpridos os aspectos definidos no Modelo de Informação, Modelo Organizacional, Modelo de Comunicação e no Modelo Funcional – apresentados na secção 2.2.2 – para que a informação seja compatível entre diferentes ferramentas e possa ser acedida através de interfaces e protocolos em comum.

Na secção 2.4.1 segue-se a apresentação e descrição das ferramentas selecionadas integradas na área de gestão e monitorização de redes e sistemas.

2.4.1. Selecção e Descrição das Ferramentas

Para a selecção das ferramentas focou-se a procura em dois grupos de ferramentas: o primeiro grupo direcionado para a gestão e monitorização de redes e o segundo grupo para a gestão de inventário.

Da pesquisa realizada sobre as ferramentas de gestão e monitorização de redes, obteve-se um valor na ordem das dezenas [32] [33]. Este último valor foi reduzido para cerca de metade, tendo-se utilizando para esse objectivo os critérios de 'custo' e o 'nível de abertura' – mencionados na secção anterior –, que permitiram excluir todas as ferramentas que não cumprissem com as principais restrições impostas pelo CCCEE, nomeadamente:

- Por não existirem recursos financeiros disponíveis, o CCCEE não poderá cobrir nenhum custo com a implementação das soluções. Deste modo, a escolha dos *softwares* tem que recair para os que adotam licença gratuita, e;
- As soluções a implementar devem ainda conseguir gerir e monitorizar os vários tipos de máquinas e sistemas operativos a funcionar na rede informática do CCCEE.

Numa nova filtragem, utilizou-se o critério de 'funcionalidades' e o de 'novas aplicações' em que se procurou por ferramentas que disponibilizavam, por exemplo: mecanismo para a obtenção e a visualização de dados, capacidade para a monitorização de serviços e recursos de diferentes equipamentos, mecanismos de detecção e notificação de problemas, e *pluggins*.

Com esta última triagem, foi possível obter um conjunto mais pequeno de ferramentas, em que se terminou por selecionar, deste último conjunto, apenas três ferramentas de gestão e monitorização de redes (Cacti, Icinga e Zabbix), número este de ferramentas que se considerou adequado para o âmbito deste projecto.

Adicionalmente, através do contacto com duas situações reais – onde foi possível observar como era realizada a gestão e monitorização de uma rede –, obteve-se a referência a três ferramentas de gestão de inventário: o OTRS (*Open-source Tickets Request System*) [34], o OCS Inventory NG (OCS), e, por fim, o GLPI (*Gestionnaire Libre de Parc Informatique*) [35].

Deste último grupo de quatro ferramentas, excluiu-se o OTRS por já se encontrar em funcionamento na rede do CCCEE como solução à gestão de *tickets*, e ainda o GLPI, por se tratar de uma ferramenta híbrida, disponibilizando as mesmas funcionalidades que o OTRS – o que duplicaria a função de *tickets* – e as tarefas de gestão de inventário, fornecidas neste caso pelo OCS Inventory NG.

Assim, segue-se uma apresentação e descrição de algumas das características das ferramentas: Cacti, Icinga, Zabbix e OCS Inventory NG, respectivamente.

CACTI

O Cacti [36] [37] pertence ao grupo de ferramentas responsáveis pela monitorização dos sistemas de uma rede, de pequenas ou grandes infra-estruturas. Tem como principal característica permitir ao utilizador visualizar e analisar a informação recolhida através de vários gráficos, apresentados na Figura 5, que posteriormente podem ser organizados numa hierarquia em árvore.

Figura 5 – Tipos de gráficos disponibilizados pelo Cacti [38]

A nível arquitetural (Figura 6), um dos principais componentes do Cacti é a ferramenta *RRDtool* [39], responsável pelo armazenamento dos dados - por exemplo, dos *routers* e/ou servidores - e pela construção de diferentes tipos de gráficos. O Cacti utiliza o protocolo SNMP e um *Poller*[1], como meios para obtenção de informação dos sistemas existentes na rede, não disponibilizando nenhum agente para configurar nas máquinas clientes (ou *hosts*). As configurações da ferramenta ficam guardadas numa base de dados *MySQL*, podendo o sistema ser gerido pelo administrador via *web browser*.

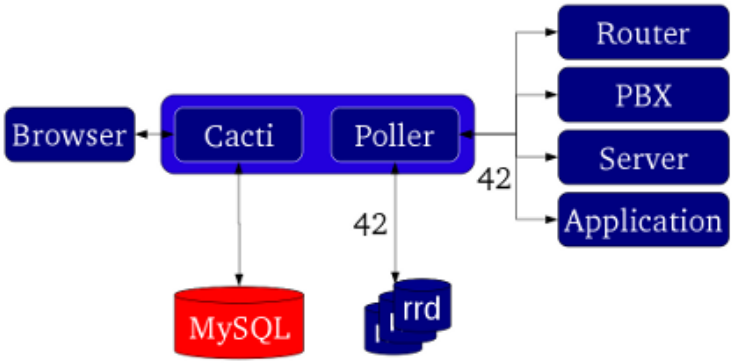


Figura 6 - Arquitectura do Cacti [40]

Após a instalação, é disponibilizado um conjunto base de funcionalidades, que permitem a um utilizador desempenhar um determinado número de tarefas, entre as quais: a configuração e visualização dos dados dos sistemas e equipamentos monitorizados, definição de *templates*, gestão dos utilizadores e algumas configurações do próprio sistema. Contudo, a plataforma do Cacti possibilita estender as funcionalidades através da adição de alguns *plugins* e, desta forma, aumentar o número de tarefas. Dos *plugins* disponibilizados, destacam-se os seguintes [41]:

- ***Discovery*** – Tem a capacidade de descobrir equipamentos e sistemas numa rede, apresentando o estado do dispositivo e do protocolo SNMP;
- ***MAC Track*** – Localiza os equipamentos na rede com base no *IP* e/ou *MAC address* e consegue ajudar a rastrear ataques como, por exemplo, vírus;
- ***Network WeatherMap*** – Possibilita a criação de diferentes mapas da rede;
- ***RouterConfig*** – Utilizado para realizar um *backup* noturno das configurações dos routers, podendo comparar e exibir as diferenças entre quaisquer duas configurações;
- ***Syslog*** – Permite, entre outras coisas, visualizar mensagens *syslog* armazenadas na base de dados;
- ***Thold*** – É o módulo principal de criação de alertas, com diferentes níveis de severidade, que são enviados por *e-mail* a um ou mais utilizadores.

[1] ***Poller*** – Trata-se de uma aplicação/*script*, que comunica com os dispositivos para recolher informações, sendo executada num intervalo de tempo constante.

ICINGA

Das ferramentas que têm por objectivo gerir e monitorizar a rede, encontra-se o Icinga [42] que foi originalmente desenvolvido através de uma bifurcação da ferramenta Nagios [43]. No artigo [44], verifica-se parte do caminho percorrido durante esta transição do Nagios para o Icinga, sendo que o lento desenvolvimento da ferramenta, a falta de melhorias tais como as ligações à base de dados e a falta de uma API (*Application Program Interface*) que facilitasse a integração de *addons* foram, entre outros, os principais factores que levaram à bifurcação. Como consequência desta bifurcação, muitas das configurações e funcionalidades do Nagios tornaram-se compatíveis com o Icinga.

Dos componentes existentes na arquitectura do Icinga, na Figura 7, o *'Icinga Core'* é o principal componente responsável por gerir as tarefas de monitorização e analisar os resultados enviados pelos *plugins*. Por sua vez, é o componente '*Icinga Web*' onde são apresentados os resultados da monitorização da rede, que permitem visualizar o estado dos serviços, o histórico, notificações e mapa de rede, entre outros. São disponibilizadas duas interfaces diferentes: o modo '*Classic UI*', com um aspecto muito semelhante ao Nagios, e o modo '*Web*', com uma aparência moderna e mais avançada em termos de usabilidade.

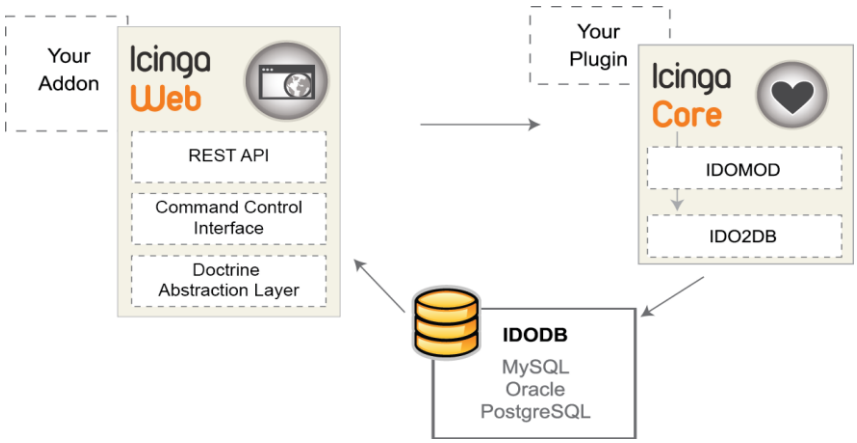


Figura 7 - Arquitectura do Icinga [45]

O administrador pode também optar por implementar apenas um único servidor para monitorizar a rede (monitorização centralizada) ou por escolher uma monitorização distribuída, em que existe um servidor central e vários outros servidores dedicados à monitorização, possibilitando desta forma uma distribuição da carga, maior segurança e redundância.

Esta plataforma utiliza o protocolo SNMP como principal meio de adquirir dados dos equipamentos e, embora não exista a obrigação de usar agentes, são disponibilizados, por exemplo, os agentes *NSClient++* [46] e *NRPE* (*Nagios Remote Plugin Executer*) [47] para os sistemas operativos *Windows* e *Linux*, respectivamente.

No entanto, para efectuar qualquer configuração no sistema ou definir *templates*, alertas, equipamentos e serviços a monitorizar, o administrador necessita de recorrer à linha de comandos e reiniciar o servidor após cada alteração nos ficheiros de configuração.

ZABBIX

O Zabbix [48] [49] é uma ferramenta dedicada à gestão de redes e monitorização de vários equipamentos e serviços, tendo adotado várias funcionalidades do Nagios e do Cacti. No entanto, ao contrário do Cacti, que não disponibiliza agentes para configurar nos *hosts*, o Zabbix recorre, não só, a um agente, mas também a outros métodos para a recolha de informações das máquinas a monitorizar, tais como:

- Protocolo SNMP;
- Mecanismos de simples verificações, utilizadas, normalmente, para monitorizarem serviços remotos que não contenham o agente;
- IPMI (*Intelligent Platform Management Interface*), que fornece dados do ambiente físico de um servidor de *hardware* como, por exemplo, a temperatura e a velocidade da ventoinha, e;
- O componente Zabbix java *gateway* denominado por JMX[2] (*Java Management Extensions*).

A arquitectura base desta plataforma, apresentada na Figura 8, é distribuída, consistindo num servidor central encarregue de administrar o sistema e de lidar com a interacção entre os outros dois componentes principais: o '*Zabbix Agent',* que monitoriza os recursos e aplicações locais e envia-os para o servidor, e o '*Zabbix Proxy'*, que embora seja uma parte opcional da configuração do Zabbix, é essencial para uma monitorização distribuída. O *zabbix proxy* recolhe os dados dos *hosts* e armazena-os numa base de dados própria de modo a evitar perda de informação caso exista algum problema com a comunicação ao servidor.

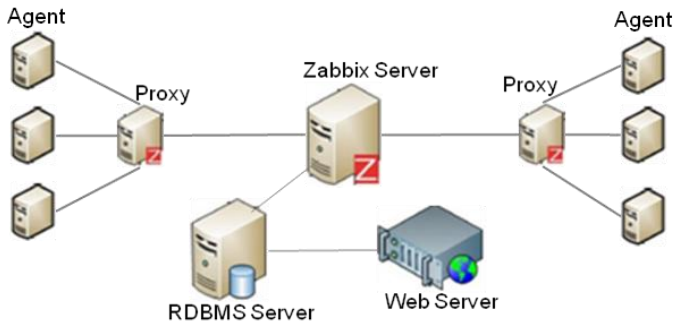


Figura 8 - Arquitectura do Zabbix [48]

O mecanismo de notificações desta plataforma permite ao utilizador configurar alertas de vários eventos, podendo associar um de seis níveis de gravidade diferentes.

O sistema de alertas incluí três canais de envio de notificações, via *e-mail*, sms e *jabber* (denominado, actualmente, por XMPP[3] - *Extensible Messaging and Presence Protocol*).

[2] **JMX** [57] – "define a aquitectura para software e gestão de redes na linguagem de programação Java. Promete eliminar a necessidade de soluções caras para a gestão de aplicativos específicos, definindo uma arquitectura que permite que mais aplicações genéricas de gestão sejam contruídas".

Ao nível da segurança, também permite atribuir diferentes permissões a cada utilizador e ainda três métodos de autenticação: *Internal*, LDAP e http. Para além disso, tem suporte para ambientes IPv4 e IPv6.

Todos os relatórios e estatísticas de dados, assim como os parâmetros de configuração, entre outros, são armazenados numa base de dados e podem ser acedidos e/ou definidos através de uma interface *WEB*.

OCS INVENTORY NG

O OCS Inventory NG (OCS) [50] enquadra-se nas ferramentas de gestão de inventário de equipamentos e *software*. Esta ferramenta recorre à utilização de um agente – o *OCS Agent* [51] – para adquirir informações de *hardware* e *software* de todos os *hosts* em que possa ser instalado. A frequência estabelecida para o contacto entre agente-servidor e entre cada actualização do inventário, pode ser definida pelo próprio administrador.

A arquitectura do OCS Inventory NG, apresentada na Figura 9, é baseada no modelo cliente-servidor e pode ser dividida em duas secções. A secção superior – *Management Server* – contém os quatro componentes principais do servidor, responsáveis por armazenar a informação dos inventários, lidar com as comunicações http e https entre o servidor e o agente, guardar as configurações e permitir aos administradores aceder ao sistema através de um *web browser*. Por sua vez, a secção inferior – *Network Agent* – abrange todo o conjunto de máquinas das quais se pretende manter o inventário, com diferentes sistemas operativos e que podem ou não se encontrar na rede.

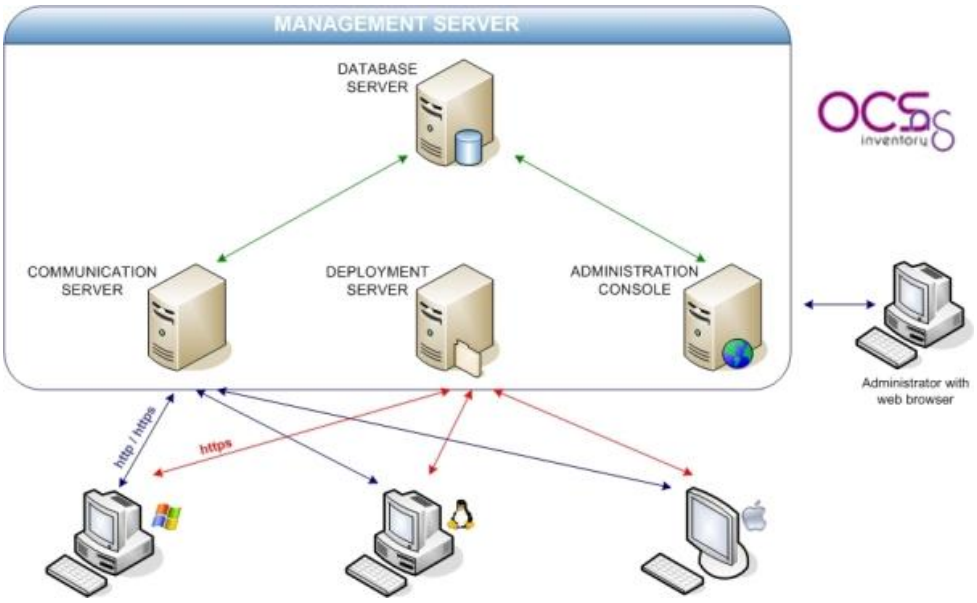


Figura 9 - Arquitectura do OCS Inventory NG [52]

Na Tabela 2 é apresentado um exemplo de um inventário de um computador, obtido através da utilização de um agente OCS.

[3] **XMPP** [58] **–** "é uma tecnologia aberta para comunicação em tempo real, usando o Extensible Markup Language (XML) como formato base para a troca de informações. Em essência, XMPP fornece uma maneira de enviar pequenos pedaços de XML de uma entidade para a outra quase em tempo real".

Tabela 2 - Dados obtidos de um computador pelo Agente OCS

TIPO	INFORMAÇÃO
Informação Geral	Nome; *Domain*; Endereço *IP*; Utilizador; *Swap*; *OS Name*; *OS Version*; *Service Pack*; Utilizador *Windows*; Licença *Windows*; Chave *Windows*; *User Agent*; Memória; *Último Inventário*; Último Contacto; Nome da Rede; *Uuid*;
Processador (es)	Tipo; Velocidade do Processador (*MHz*); Quantidade;
Memória	*Caption*; Descrição; Capacidade (*MB*); *Purpose*; Tipo; Velocidade; Número de *Slots*; Número de Série;
Armazenamento	Nome; *Manufacturer*; Modelo; Descrição; Tipo; Tamanho do Disco (*MB*); Número de Série; *Firmware*;
Disco (s)	Letra; Tipo; Designação; Sistema de Ficheiros; Capacidade Total e Disponível (*MB*);
Placa de Vídeo	Nome; *Chipset*; Memória (*MB*); Resolução;
Som	Nome; *Manufacturer*; Descrição;
Rede (s)	Descrição; Tipo; Velocidade; MAC *address*; Estado; Endereço *IP*; *Netmask*; *Gateway*; *Network number*; DHCP IP;
Controlador (es)	Tipo; *Caption*; Descrição; Versão;
Slot (s)	Nome; Descrição; Designação;
Porta (s)	Tipo; Nome; Interface, Descrição;
Bios	Número de Série; *Manufacturer*; Modelo; Tipo; *BIOS Manufacturer*; Versão; Data; *Asset TAG*;
Software	Editor; Nome; Versão; Comentários;
Monitor (es)	*Manufacturer*; *Caption*; *Manufacturer on (week/year);* Tipo; Número de Série;
Dispositivo (s) de Entrada	Tipo; *Manufacturer*; *Caption*; Descrição; Interface;
Impressora (s)	Nome; *Driver*; Porta; Descrição;

Cada *host* registado na aplicação poderá ser adicionado a determinados grupos estáticos e/ou dinâmicos. Nos estáticos, as máquinas são introduzidas e removidas desse mesmo grupo, apenas por acção do utilizador. Por sua vez, para os dinâmicos, esse processo é realizado automaticamente pela ferramenta.

O OCS integra também a tarefa de autodescobrir equipamentos, através da função '*IPdiscover'* [53] que encontra os equipamentos mesmos protegidos pela *firewall*, e através do protocolo SNMP. Esta funcionalidade possibilita manter um inventário para dispositivos como impressoras ou *switches*, onde não é possível configurar um agente.

Através da implementação de *plugins*, é ainda possível adicionar novas funcionalidades, por exemplo, saber o tempo de actividade de um computador (*Retrieve Machine Uptime*), a versão e o estado do Antivírus/*Anti Spywares*/*Firewall* (*Retrieve Security informations*), as informações sobre o estado dos serviços e processos (*Retrieve Services* e *Retrieve Running Processes*), assim como gerir as licenças do Office (*ManageMSofficeKey* e *Retrieve Microsoft Office key*) [54].

No entanto, não é disponibilizado pela ferramenta um sistema de alertas e/ou notificações, mas o administrador tem a possibilidade de atenuar esta lacuna com a instalação de outros *softwares*, como por exemplo a ferramenta GLPI [55].

No capítulo 4, secção 4.2, será realizada uma comparação das funcionalidades das ferramentas selecionadas e apresentadas na presente secção.

2.5. Conclusão

Neste capítulo efectuou-se um estudo das cinco áreas funcionais em que a gestão de redes foi dividida e realizou-se a análise das tradicionais arquitecturas de gestão, de modo a se conhecer o funcionamento da interacção e comunicação entre os sistemas numa rede de TI, i.e., conhecer quais os mecanismos existentes que possibilitam gerir e manter uma rede operacional.

Através de uma breve análise aos modelos ITIL e FCAPS, verifica-se que o FCAPS contém muitos dos recursos críticos necessários para a gestão e operacionalidade, enquanto o ITIL é projectado na forma de orientação sobre processos e métodos para a gestão das TI de uma organização.

Um ponto essencial é que, embora existam cinco áreas no modelo FCAPS, uma pode influenciar o sucesso de outra. Por exemplo, na ocorrência de problemas de falhas, de configuração ou de desempenho, estas situações poderão estar encobertas por problemas relacionados com a segurança. Por outro lado, também se verificou que é importante identificar quais as áreas funcionais que é mais crucial abordar na solução de gestão a implementar.

A nível das ferramentas de gestão e monitorização de redes pode-se afirmar que o leque de ferramentas disponíveis no mercado é consideravelmente grande, tornando o processo de comparação e selecção dessas ferramentas uma tarefa demorada. Uma vez que, para a rede informática do CCCEE, numa perspectiva a médio e longo prazo, a previsão é para um lento crescimento da rede, não sendo por isso esperadas grandes alterações na aquisição de novas tecnologias de informação para o CCCEE, os critérios de ‘extensibilidade’ e ‘actualização tecnológica’ tiveram pouca (ou nenhuma) influência num primeiro processo de selecção das ferramentas mais relevantes.

3. Gestão de Sistemas e Serviços do CCCEE

3.1. Introdução

No capítulo actual, o Centro de Competências de Ciências Exactas e da Engenharia (CCCEE) apresenta-se como o ambiente de trabalho do presente projecto. Como cada infra-estrutura informática contém as suas próprias características, é importante fazer a análise e o levantamento de informações sobre a rede informática em questão, antes da implementação de um sistema de gestão e monitorização, para que seja possível identificar os seus requisitos como, posteriormente, identificar os pontos críticos que precisam de uma intervenção mais rápida.

Na primeira parte deste capítulo, inicia-se com uma caracterização geral do CCCEE, identificando-se e descrevendo-se os seus utilizadores, as principais características relacionadas com a rede e serviços, assim como os recursos de *hardware* e *software* existentes no campus informático do CCCEE.

Na segunda e última parte do capítulo, termina-se com uma análise à gestão das tecnologias de informação do CCCEE, fazendo o levantamento dos problemas encontrados em toda a infra-estrutura informática e identificando-se os principais necessidades e requisitos do CCCEE na área de gestão de TI.

3.2. Descrição do CCCEE

O Centro de Competências de Ciências Exactas e da Engenharia (CCCEE) pertence à estrutura da Universidade da Madeira (UMa) e situa-se no Campus da Penteada. Neste Centro são desenvolvidas actividades de ensino e investigação nos três ciclos de ensino superior, nas áreas da Física, Engenharia Civil e Geologia, Engenharia Eletrotécnica, Engenharia Informática, Design de Média Interactivos, Matemática e Química.

As instalações do CCCEE distribuem-se por vários pisos do edifício da UMa e incluem os gabinetes de docentes, os espaços reservados aos Centros de investigação, as salas de aulas e os laboratórios, os espaços para armazenamento e arquivos, assim como salas de estudo e salas de reuniões multiuso.

Entre os utilizadores que utilizam os serviços do Centro fazem parte todos os alunos da Universidade da Madeira, professores, investigadores e funcionários. Em geral, os utilizadores podem ser organizados em dois grupos principais: o grupo dos alunos e o grupo dos funcionários (denominado daqui para a frente como grupo dos docentes) que integra todos os professores, investigadores e funcionários do CCCEE.

Nas instalações do CCCEE existem serviços informáticos e de suporte que são suportados pelo Sector de Comunicações e Informática (SCI) da Universidade da Madeira e outros que são geridos pelo próprio CCCEE.

Na rede de computadores existe também uma grande variedade de tipos de equipamentos que são direccionados para a área da investigação e outros para as actividades de ensino e que podem ser associados às seguintes categorias: dispositivos de acesso à rede, dispositivos de interligação de redes, dispositivos de segurança, sistemas terminais (servidores e postos de trabalho) e dispositivos periféricos (entrada, saída e de armazenamento).

Na secção seguinte, descrevem-se os utilizadores e os recursos de *hardware* e *software* do CCCEE, com grande ênfase na respectiva rede e sistemas de informação. Os dados aqui apresentados foram cedidos pelo responsável pelo Centro, à data da escrita deste documento.

3.2.1. Utilizadores do Centro

Como membros do CCCEE existem cerca de seis centenas de alunos, divididos entre as várias áreas científicas e os diferentes ciclos de ensino superior, vários funcionários e perto de setenta professores e investigadores a integrar o corpo docente.

Todos os utilizadores pretendem aceder à rede informática e usufruir dos serviços fornecidos. O grupo de alunos e docentes tem, em comum, várias necessidades relativas à utilização dos serviços, entre as quais aceder e utilizar os serviços da Internet, de impressão e de e-mail, obter as licenças para os *softwares*, e ainda necessitam que os programas e aplicações de apoio às aulas, por exemplo o *Mathematica* e o *MatLab*, estejam instalados nos computadores das salas de aulas e em laboratórios, assim como de ter os respectivos equipamentos funcionar correctamente.

A responsabilidade de garantir o correcto funcionamento da rede, a disponibilidade dos serviços fornecidos aos utilizadores e os *backups* dos servidores, está a cargo apenas de um único administrador de redes, existindo ainda o apoio local de um técnico de laboratório, encarregue das seguintes funções:

- Gestão do servidor de licenças dos *softwares* (pagamento, instalação e actualização das licenças);
- Produção de um manual de instalação para alunos e técnicos de informática que vão instalar os *softwares* nas salas de aula (salas de informática);
- Gestão e manutenção do servidor de *e-mail* do CCCEE;
- Reparação de equipamento das salas de aula de Eletrónica e Telecomunicações;
- Ajuda na utilização de serviços fornecidos aos respectivos membros;
- Compilação da lista de necessidades dos laboratórios (componentes, reparações e equipamentos), e;
- Consulta de fornecedores e acompanhamento de aquisições.

Aos gestores de rede são ainda atribuídas outras tarefas, para auxiliar os diferentes grupos de utilizadores do CCCEE (alunos e docentes), como por exemplo:

- **Alunos**:
  - Acessos a laboratórios de *hardware*;
  - Apoio na Instalação de *Software* de Engenharia e Matemáticas: SPSS, *Mathematica*, *Matlab*, *Labview*, etc;
  - Fornecimento das licenças *Microsoft* MSDNAA e ajuda na criação de novas contas e na renovação e recuperação de senhas;
  - Fornecimento das licenças do *software Mathematica*, aceitação de novas contas e ajuda na recuperação das chaves do produto;
  - Impressão de *posters* para a apresentação de projetos;
  - Ajuda na configuração da rede sem fios;
  - Criação de espaço *web* nos servidores do CCCEE para publicação de páginas *web*;
  - Empréstimo de material de eletrónica e telecomunicações (componentes e equipamento);
  - Formação e acompanhamento na utilização dos componentes e equipamentos, e;
  - Formação e acompanhamento na produção de circuitos impressos.

- **Docentes**:
  - Disponibilização de componentes ou equipamentos para uma aula ou projeto específico;
  - Preparação das aulas práticas (colocação dos componentes e equipamentos necessários à aula e também na preparação de pequenos circuitos eletrónicos para aulas);
  - Instalação e/ou configuração de *kits* didácticos;

- Ajuda na utilização dos serviços disponibilizados, e;
- Configuração da rede sem fios nos equipamentos.

Como consequência da actual escassez de recursos humanos para gerir todo o campus informático do CCCEE, as respostas a esses pedidos de apoio são, em muitas das situações, tardias e demoradas.

Na secção seguinte descrevem-se as características da rede que cobre o CCCEE.

3.2.2. Rede

O núcleo da rede do CCCEE situa-se no piso 2 da Universidade da Madeira. Nesta área existe uma zona técnica reservada ao alojamento dos distribuidores e dos bastidores, onde estão instalados os equipamentos activos e passivos – na sua maioria para a rede dos docentes –, entre outro material importante para o funcionamento da rede. Existem também alguns bastidores nos laboratórios que têm o objectivo principal de apoiar as aulas lá leccionadas. A rede informática que suporta a interligação entre todos os equipamentos e a ligação destes à restante rede da UMa e à Internet é da responsabilidade do SCI.

As instalações do CCCEE são cobertas por duas VLANs: VLAN dos alunos e VLAN dos docentes, apresentado na Figura 10. Ambas as VLANs operam sob a tecnologia Ethernet e utilizam a seguinte gama de endereços IP: 10.1.2.X e 10.1.222.X, para a rede dos docentes, e 10.2.15.X, para a rede dos alunos.

As políticas de segurança na rede do CCCEE, aplicadas pelo SCI para a rede da UMa em geral, restringem a interacção entre sistemas que não estejam na mesma rede, à excepção, por exemplo, de alguns serviços web como o Moodle, que precisam de ser acedidos pelos alunos e docentes do CCCEE.

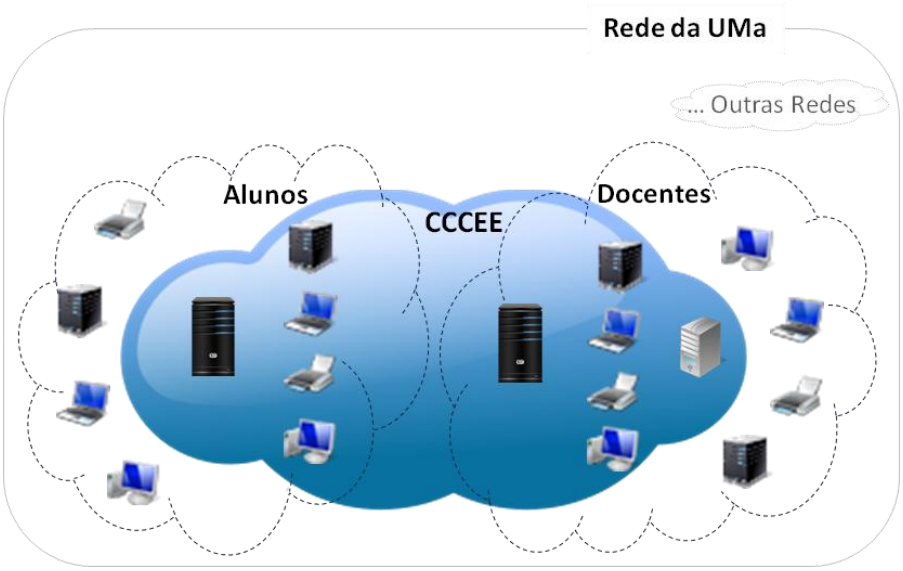


Figura 10 - Esquema geral da rede do CCCEE

Os recursos informáticos do CCCEE integram vários equipamentos que pertencem às classes de interligação, como *Routers*, e de acesso à rede, como: Switches, *Multi-layer Switches* e, ainda, vários *Access Points* que possibilitam aos utilizadores do CCCEE se ligarem à rede local através de ligações sem fios (*Wi-fi*), sendo que a gestão desta rede sem fios fica a cargo do SCI.

As falhas no acesso à rede ocorrem com alguma frequência e com uma duração variável, tornando impossível usufruir do acesso aos diferentes serviços disponibilizados aos membros do CCCEE, durante a ocorrência das falhas. Como perspectiva de futuro, não estão previstas grandes alterações no desenvolvimento e crescimento da rede.

Na próxima secção dá-se seguimento à descrição dos serviços fornecidos aos vários membros do CCCCEE.

3.2.3. Servidores e Serviços

No CCCEE, encontram-se em funcionamento vários servidores, apresentados na Tabela 3, dos quais alguns estão alojados em ambientes virtuais, em equipamentos cujo estado físico limita o estado dos serviços e, consequentemente, o seu bom funcionamento e desempenho. Por este motivo, ocorrem falhas constantes na disponibilidade dos vários serviços, sendo comum que, por diversas vezes, os gestores da rede só tomem conhecimento destas situações após a existência de alguma reclamação por parte dos utilizadores.

Tabela 3 - Servidores WEB utilizados no CCCEE

Servidor WEB		Descrição
AcademiaCisco	academiacisco.cee.uma.pt	Plataforma moodle para a Academia Cisco/UMa;
Apoio	apoio.cee.uma.pt	Páginas com documentação de apoio técnico diverso;
Apus	apus.uma.pt	Servidor para projectos de alunos de mestrado (utilizado principalmente pela área das redes de computadores);
CCM	ccm.uma.pt	Página do Centro de Ciências Matemáticas (CCM);
CEESOFTKEYS		Gestor de licenças de rede para diversos *softwares*.
DEI	dei.cee.uma.pt	Página para o Doutoramento em Engenharia Informática;
Droid	cee.uma.pt/droid2	Página do projecto Droid2;
Inventário	cee.uma.pt/inventario	Página com a listagem dos equipamentos e alguma informação de aquisições para os laboratórios de *hardware;*
Moold	moold.cee.uma.pt/<Anos>	Histórico dos diversos anos lectivos do Moodle;
Moodle	moodle.cee.uma.pt	Plataforma para suporte às disciplinas lecionadas pelo CCCEE;
Moodle2	orion.uma.pt/moodle2	Plataforma Moodle de teste e desenvolvimento;
Open Ticket Request System		Sistema de gestão de *tickets*;
Página do Centro	cee.uma.pt	É o rosto do Centro e contém a apresentação dos cursos, divulgação de notícias, actividades, fóruns e informação dos membros do Centro, servindo ainda para disponibilizar as fichas das disciplinas necessárias por os processos da A3ES. Muita desta informação está desatualizada;
Página do Centro na UMa	ccee.uma.pt	Com o propósito anterior (contudo, ainda mais desatualizada);

Na Tabela 4, por sua vez, são apresentados alguns dos principais serviços existentes e disponibilizados para todos os elementos do Centro.

Tabela 4 - Serviços Disponibilizados pelo CCCEE

Serviço		Descrição
E-mail	Centro (<user>@cee.uma.pt)	Alojado num servidor do próprio Centro;
	UMa (<user>@uma.pt)	Serviço fornecido pela UMa para todos os membros;
Área de Ficheiros Central	(\\10.1.222.253 ou \\storage)	Para armazenamento e salvaguarda de ficheiros;
Área para Página Pessoal	(\\10.1.222.253\user\www)	Com possibilidade de ligação a uma base de dados;
e-Learning Moodle	(http://moodle.cee.uma.pt)	Plataforma para a disponibilização de conteúdos das disciplinas;

Existem, ainda, outros serviços que, por estarem descontinuados e desactualizados não são aqui mencionados, mas que necessitam ser mantidos e, por vezes, actualizados.

De seguida, apresentam-se os diferentes recursos de *hardware* e *software* que existem e estão disponíveis nos vários espaços das instalações no CCCEE, para os vários utilizadores.

3.2.4. Recursos de *Hardware* e *Software*

Nos espaços para as actividades de ensino e de investigação, assim como nos gabinetes dos docentes, existe à disposição dos diversos membros do CCCEE um conjunto de equipamentos, como por exemplo:

- **Sistemas Terminais**:
  - É fornecido pelo CCCEE um computador a cada um dos cerca de setenta professores (embora muitos decidam utilizar o seu próprio computador pessoal, nomeadamente um portátil), e;
  - Em cada espaço de salas de aulas e laboratórios, existem perto de vinte computadores instalados sob responsabilidade do SCI; contudo, alguns destes equipamentos apresentam alguma degradação, e consequentemente, necessitam de manutenções frequentes.

- **Periféricos de Saída (*output*)**:
  - Várias impressoras (algumas nos próprios gabinetes dos docentes) e uma *plotter.* Estas possibilitam as funcionalidades de fotocopiar, imprimir e, ainda, de fax. A ausência de recursos para as mesmas funcionarem é notificada frequentemente aos gestores da rede do CCCEE pelos próprios utilizadores destes serviços;

- Por regra, um projector em cada espaço para as actividades de ensino, e;
- Outros periféricos como: colunas e monitores de computadores.

➢ **Periféricos de Entrada (*input*)**:

- Teclados, ratos, microfones e *webcams*;

Outros equipamentos como computadores, monitores, ratos e até impressoras, permanecem armazenados/depositados em alguns espaços de arrumos. Alguns aguardam por alguma reparação e outros, por razões diferentes, encontram-se sem condições para funcionarem correctamente, sendo reaproveitados os componentes que ainda se encontram em bom estado para reparar outros equipamentos.

Quanto ao *software*, a tecnologia utilizada para suportar os diversos equipamentos existentes na rede assenta predominantemente no Sistema Operativo *Windows*, existindo uma pequena percentagem de sistemas que não pertencem à família da *Microsoft*, como em particular em alguns servidores que têm instalado o Sistema Operativo *Linux* e, ainda, os ambientes virtuais (*VMWare ESXi* e *Citrix XenServer*). Encontram-se diversas versões dos sistemas operativos em funcionamento, facto que resulta dos mesmos estarem normalmente associados ao período de tempo de aquisição do equipamento.

Os sistemas operativos e aplicações disponíveis e instaladas nos vários equipamentos são muito variados e com licenças de diversos tipos, desde licenças gratuitas por tempo ilimitado até licenças pagas com renovações anuais. A manutenção das licenças não tem um controlo apertado, originando situações em que os sistemas operativos ou as aplicações deixam de poder operar por não terem sido realizadas atempadamente as renovações necessárias das licenças. Dos *softwares* com licenças comerciais, destacam-se: *Wolfram Mathematica*, *MathWorks MatLab*, *ComSol Multiphysics*, *LabVIEW*, *MultiSIM*, *IBM SPSS* e, por fim, o *MSDNA.*

Tendo-se apresentado as características e a estrutura da rede informática do Centro de competências de Ciências Exactas e da Engenharia, apresentam-se de seguida os problemas identificados e detectados na área da gestão das tecnologias de informação.

3.3. Análise à Gestão das TI do CCCEE

Numa primeira análise aos dados apresentados na secção anterior, sobressai a ausência de uma metodologia aplicada no campus informático do CCCEE, que possibilite seguir um plano de monitorização e gestão de todos os componentes e sistemas da rede, para que os gestores consigam obter um conhecimento em relação ao estado actual dos serviços de tecnologias de informação fornecidos aos membros do Centro.

Constata-se, frequentemente, problemas de acesso à rede, que implicam que a utilização dos serviços, por parte dos utilizadores, fique comprometida. Além disso, – e embora a rede sem fios não seja gerida pelo CCCEE – verifica-se, ocasionalmente, alguns congestionamentos na rede sem fios tornando o uso da mesma impraticável.

Relativamente ao *hardware* e *software*, não existem informações sobre que sistemas existem em cada espaço de actividades de ensino e investigação, nem um controlo na actualização dos sistemas operativos e das aplicações configuradas nos equipamentos.

Adicionalmente, por ocorrerem avarias constantes nos computadores integrados nesses espaços, muitos alunos optam por utilizar os seus próprios computadores pessoais durante as aulas.

As insuficientes condições físicas e lógicas dos servidores e das máquinas virtuais (VMs) que alojam alguns serviços do CCCEE comprometem, não só a disponibilidade desses mesmos serviços, como prejudicam o normal funcionamento de todas as actividades desenvolvidas pelo Centro.

Outro problema é as constantes reclamações relativamente à ausência na reposição de recursos essenciais para os equipamentos funcionarem como, por exemplo, de papel e tinteiros para as impressoras.

Identificam-se, ainda, problemas na verificação das licenças adquiridas para os *softwares* funcionarem, podendo haver situações em que estejam a ser pagas licenças de aplicações já disponíveis e outras situações em que os *softwares* não podem funcionar por não terem sido renovadas as respectivas licenças dentro do período de tempo estabelecido.

De referir também que, por não existirem *backups* de todos os serviços alojados nos servidores do CCCEE, na ocorrência de uma avaria de algum dos servidores, o normal funcionamento desses serviços poderá ser afectado.

O inventário de todos os componentes de *hardware* e *software* sob responsabilidade do CCCEE encontra-se desatualizado, sendo o registo de cada componente inserido individual e manualmente num servidor *web*, abrangendo maioritariamente os registos do *hardware*, sendo que os dados de *software* abrangem apenas, de forma incompleta, a informação das respectivas licenças.

Em redes com as dimensões semelhantes às do CCCEE, as tarefas de gestão e monitorização dos diversos sistemas a operar na rede, deveriam ser distribuídas por mais do que uma pessoa. Contudo, esta condição não é o que se verifica na prática em vários ambientes reais, incluído a própria rede do CCCEE.

Adicionalmente, por diversas vezes, os próprios gestores da rede não conseguem reconhecer rapidamente a causa dos problemas que afectam o funcionamento dos equipamentos e a indisponibilidade dos serviços, tendo que dispensar períodos de tempo extraordinários para conseguirem identificar o que provocou as falhas no sistema informático do CCCEE.

Na próxima secção faz-se o levantamento das principais necessidades existentes, face aos problemas detectados no campus informático do CCCEE.

3.3.1. Especificação de Requisitos

Pela análise aos problemas descritos na secção anterior, destaca-se a importância de implementar um modelo de gestão de redes e sistemas, que ajude na execução de estratégias para melhorar a qualidade e a eficiência dos serviços prestados aos utilizadores do Centro.

Esse modelo deve, entre outros casos, permitir que os responsáveis pela administração/gestão do campus informático do CCCEE tenham conhecimento de que papel e que tarefas lhes são atribuídos, para que a pessoa certa saiba quando, onde e como agir numa determinada situação, segundo as normas pré-estabelecidas.

Uma vez que não é possível eliminar a condicionante da falta de recursos humanos para garantir uma melhor qualidade de respostas aos pedidos de ajuda aos utilizadores, existe portanto a necessidade de adquirir uma solução integrada que possibilite uma visão do estado de toda a infra-estrutura informática do Centro, com o objectivo dos gestores de rede conseguirem intervir de forma mais expedita sobre os problemas.

Verifica-se também que, por se tratar de uma rede direcionada para as actividades de ensino e investigação, um dos principais desafios será garantir o bom desempenho da rede e a disponibilidade de todos os recursos e serviços necessários para o correcto funcionamento das respectivas actividades.

Deste modo, devem ser geridos e monitorizados – quer na rede dos alunos quer na dos docentes – o estado dos servidores que alojam os vários serviços do CCCEE, os próprios serviços e todos os equipamentos sob responsabilidade do Centro.

Assim, relativamente ao *hardware,* os parâmetros a monitorizar, por exemplo, nos computadores e servidores – independentemente do sistema operativo –, deverão abranger os seguintes componentes:

- Disponibilidade do sistema;
- Carga e utilização do processador;
- Quantidade de memória total e disponível;
- Quantidade de tráfego de rede;
- Temperatura;
- Espaço disponível e percentagem de utilização do disco;

Por sua vez, da monitorização dos *routers* e *switches* deverá resultar a informação do estado das portas, do tráfego de rede em cada interface e o número de falhas de comunicação.

O principal requisito das impressoras é ser possível ter o conhecimento do nível dos tinteiros/*toners* e a quantidade de papel, para evitar com antecedência a falta de recursos, na situação de ser pretendido utilizar o serviço de impressão.

A nível dos processos e serviços, pretende-se obter a informação do número total de processos a operar num sistema, bem como do estado (iniciado, pausa e parado) dos seguintes tipos de serviços: DHCP, DNS, FTP, IMAP, LDAP, POP, SMTP, SNMP, SSH e Telnet.

Os gestores da rede do CCCEE deverão também ser alertados quando os vários tipos de parâmetros monitorizados, por exemplo, dos diferentes componentes de *hardware ou serviços* – mencionados anteriormente –, atinjam ou estejam na eminência de atingir determinadas percentagens/valores que possam ser considerados críticos para uma dada situação.

Nos *softwares*, uma vez que nas instalações no CCCEE são realizadas não só actividades de investigação como também de ensino, é importante garantir que as aplicações necessárias para que os alunos possam acompanhar a matéria das aulas estejam configuradas nos computadores dos respectivos espaços e a funcionar correctamente, bem como manter um registo actualizado dos softwares instalados.

Devido ao método de inventário utilizado se traduzir num processo moroso, exigindo que cada dado seja inserido individualmente no sistema, a informação existente – acerca dos vários componentes de *hardware* e *software* e da informação das novas aquisições para o Centro – encontra-se bastante desatualizada. O objectivo será, então, eliminar esta condicionante, i.e., de ter que inserir cada dado dos diferentes componentes manualmente no sistema, e, por outro lado, adquirir dados mais completos dos equipamentos.

Em suma, como o CCCEE apresenta uma diversidade de serviços e de componentes de *hardware* e *software* – quer com diferentes características quer com diferentes condições respectivamente ao grau de conservação e funcionamento – deve ser realizada uma gestão e monitorização adequada a cada equipamento ou componente. Para além disso, a monitorização dos servidores e serviços fornecidos pelo CCCEE, é vista como uma parte prioritária por parte dos gestores da rede do CCCEE.

3.4. Conclusão

No presente capítulo deu-se a conhecer um conjunto de informações acerca da infra-estrutura informática do CCCEE, que se apresentou como um cenário diversificado em sistemas, serviços, tecnologias e aplicações, com uma série de características particulares. O levantamento de toda a informação foi realizada através de várias entrevistas ao actual administrador da rede do CCCEE. Com estas informações, foi possível perceber que existe a necessidade de adoptar e implementar um modelo e um sistema de gestão e monitorização de TI, a fim de melhorar a qualidade de actuação aos problemas detectados e a qualidade dos serviços disponibilizados aos utilizadores do CCCEE.

Por fim, com as informações obtidas neste capítulo, conseguiu-se também definir que tipos de problemas existem no CCCEE e, ainda, quais os equipamentos e serviços que devem ser abrangidos pelo sistema de gestão e monitorização a implementar no campus informático do CCCEE.

4. Análise e Implementação de uma Solução de Gestão

4.1. Introdução

A ideia central deste projecto prende-se com o estudo e implementação de uma plataforma integrada para a gestão e monitorização da rede do Centro de Competências de Ciências Exactas e da Engenharia, da UMa.

De um modo geral, todas as organizações têm tamanhos, características, estruturas e objectivos diferentes, não existindo consequentemente duas organizações iguais. Assim, mesmo que se verifique que uma solução funciona numa organização específica, tal não significa que essa solução poderá também ser adequada a todas as outras organizações.

As boas ferramentas de monitorização fornecem-nos valores concretos e representações gráficas do estado da rede, que ajudam a visualizar exactamente o que está a acontecer, permitindo verificar a saúde da rede e diagnosticar/resolver problemas que possam estar a ocorrer ou na iminência de acontecer.

Neste capítulo descreve-se o processo de escolha das ferramentas para a monitorização da rede do CCCEE, bem como a arquitectura da solução implementada para a gestão dos vários sistemas a operar na infra-estrutura informática do CCCEE, de modo a responder aos problemas identificados no capítulo anterior.

4.2. Escolha das Ferramentas

A escolha das ferramentas para a gestão e monitorização de redes, a implementar no campus informático do CCCEE, teve como base o grupo de ferramentas: Zabbix, Icinga e Cacti, que foram selecionadas anteriormente no capítulo 2 na secção 2.4.1 Selecção e Descrição das Ferramentas. Contudo, pelo facto do administrador e o técnico de laboratório não poderem se dedicar totalmente à gestão da rede, pretende-se que o número de ferramentas a implementar seja reduzido ao mínimo.

Desta forma, construiu-se a Tabela 5, com base em [32], para permitir uma comparação mais simples entre as funcionalidades disponibilizadas por cada uma das três ferramentas mencionadas no parágrafo anterior. Para tal, organizaram-se as diferentes funcionalidades em oito grupos (*Data Collection*, *Funcionality*, *Monitoring*, *Organizational*, *Operation*, *Problem Detection*, *Security* e *Visualization*).

Tabela 5 - Comparação de funcionalidades das Ferramentas (baseado em [32])

	FEATURES	ZABBIX	ICINGA	CACTI
Data Collection	*Agent*	✓	✓	×
	Agentless	✓	✓	✓
	SNMP	✓	✓	✓
Functionality	*Auto Discovery*	✓	*Plugin*	*Plugin*
	Distributed Monitoring	✓	✓	✓
	Inventory	✓	*Plugin*	*Plugin*
	Plugins	✓	✓	✓
Monitoring	*Monitoring Host Resources (CPU, Disk, …)*	✓	✓	✓
	Monitoring Network Services (http, ssh, …)	✓	✓	✓
Organization	*Logical Grouping*	✓	✓	✓
	Templates	✓	*Limited*	✓
Operation	*License*	*Open Source*	*Open Source*	*Open Source*
	Operating Systems	*Linux Windows*	*Linux Windows*	*Linux Windows*
	Opening Level	✓	✓	✓
	WebApp	✓	*Limited*	✓
Problem Detection	*Alerts / Notifications*	✓	✓	*Plugin*
	Real-Time Checks	✓	✓	✓
	Severity Levels	✓	✓	*Plugin*
	Trend Prediction	×	×	✓
	Historical	✓	✓	✓
Security	*Access Control*	✓	✓	✓
	Authentication	✓	✓	✓
Visualization	*Graphs*	✓	✓	✓
	Maps	✓	✓	*Plugin*

No primeiro grupo de funcionalidades, ***'Data Collection'***, todas as ferramentas utilizam o protocolo SNMP para a obtenção de dados e são capazes de monitorizar os *hosts* sem recorrer obrigatoriamente a um agente. No entanto, o Cacti é a única ferramenta que não disponibiliza qualquer agente para instalar nos *hosts* a gerir.

No grupo ***'Functionality'***, as três ferramentas suportam uma monitorização distribuída e a adição de novas funcionalidades através de *plugins*, como é o caso do Icinga e do Cacti, que

necessitam de utilizar *plugins* para as funções de descoberta automática de equipamentos bem como para realizar inventário dos sistemas.

Relativamente ao grupo ***'Monitoring'***, todas as ferramentas disponibilizam as funcionalidades de monitorização dos recursos, tanto de *software* como de *hardware*.

No quarto e quinto grupo, ***'Organization'*** e ***'Operation'***, o Icinga destaca-se pela negativa das outras duas ferramentas por não suportar as funções de *Export*/*Import* de *Templates*, e pela sua *interface web* apenas permitir visualizar os dados e efectuar pequenas interacções. Contudo, as três ferramentas conseguem gerir e monitorizar os sistemas operativos *Windows* e *Linux*, assim como diferentes tipos de equipamentos (*Opening Level*).

Do grupo ***'Problem Detection',*** as ferramentas Zabbix e Icinga não integram a funcionalidade de prever tendências (*Trend Prediction*); no entanto, as três ferramentas conseguem fornecer o histórico dos dados ao longo do tempo (*Historical*).

Por fim, no sétimo e oitavo grupo, ***'Security'*** e ***'Visualization'***, as três aplicações fornecem métodos de segurança (*Access Control* e *Authentication*) e de visualização de dados em gráficos e criação de mapas da rede.

Através de uma comparação às funcionalidades apresentadas na Tabela 5, verifica-se que as três ferramentas não possuem vantagens significativas, umas relativamente às outras, uma vez que integram em comum, um conjunto de funções muito semelhantes entre si.

Por esta razão, todas as ferramentas – Cacti, Icinga e Zabbix, incluindo ainda o OCS Inventory NG – foram efectivamente instaladas e integradas na rede do CCCEE, com o objectivo de analisar e comparar o funcionamento e desempenho das ferramentas numa situação real. Tendo-se obtido, após um intervalo de tempo de cerca de dois meses, as seguintes conclusões sobre cada uma das quatro ferramentas:

CACTI

- ✓ O Cacti permite organizar a informação monitorizada dos vários *hosts* em estruturas de árvores hierárquicas, disponibilizando várias opções de gráficos para a visualização e análise dessas informações.

- ✓ O Cacti trabalha com base na adição de vários *plugins*, o que disponibiliza por exemplo, um conjunto de várias funcionalidades complementares à ferramenta.

- × Cada *plugin* contém uma determinada função associada, e consequentemente o seu próprio método de configuração, aumentando assim, o nível de complexidade do processo de configuração – tanto da ferramenta, como da monitorização da rede – proporcionalmente ao número de *plugins* utilizados.

- × Além do exposto no parágrafo anterior, a utilização maioritariamente de *plugins* poderá acarretar problemas na compatibilidade de versões entre a própria ferramenta Cacti e o *plugin* em questão; tornando este método de extensão de funções complexo e limitado.

ICINGA

- ✓ A primeira impressão respectivamente à ferramenta Icinga é que a mesma apresenta uma interface agradável, disponibilizando ao utilizador uma visão global do estado dos sistemas e equipamentos que se encontram a ser monitorizados.

- ✓ Outra característica desta ferramenta é que ela cria automaticamente um mapa da rede com a informação do estado dos sistemas e equipamentos definidos.

- × Esta ferramenta distinguiu-se, pela negativa, pela necessidade de utilização da linha de comandos para realizar qualquer tipo de configuração (por exemplo, na definição e ou alteração dos dados de qualquer *host* a monitorizar), tornando o processo de configuração uma tarefa demorada.

- × Outro aspecto a realçar é a necessidade de, após realizar qualquer alteração nos ficheiros de configuração, ser obrigatório reiniciar o serviço do Icinga. Caso o comando não o seja executado, poderão existir incoerências nos dados relativos aos sistemas e equipamentos monitorizados.

ZABBIX

- ✓ O Zabbix permite agrupar em um único ecrã informações de várias fontes como, por exemplo: textos simples, gráficos e mapas, possibilitando desta forma uma visualização mais rápida do estado dos *hosts* monitorizados;

- ✓ O Zabbix fornece outros mecanismos, além do SNMP e do agente Zabbix, para recolher e monitorizar dados de diferentes máquinas de uma rede informática, como por exemplo: o JMX e o IPMI.

- ✓ Embora a ferramenta esteja preparada para a incrementação de novas funcionalidades através na adição de *plugins/addons*, notou-se não ser necessário recorrer a tal opção. Por exemplo, o Cacti e o Icinga necessitavam de *plugins* para a descoberta automática de sistemas na rede e para criar o inventário, e o Zabbix não.

- × A funcionalidade de detecção de '*flappings*' (i.e., detectar automaticamente a oscilação frequente do estado de um sistema) não é disponibilizada pela ferramenta, ao contrário do que acontece por exemplo com a ferramenta Icinga, o que poderá acarretar um número significativo de notificações enviadas ao administrador.

- × A função de inventário não se apresentou eficiente por exigir a definição de diferentes regras para obter diferentes dados dos *hosts* monitorizados.

OCS INVENTORY NG

- ✓ Esta ferramenta revelou-se ser simples de trabalhar e principalmente de configurar, sendo apenas necessário despender, numa fase inicial, algum tempo com a instalação dos agentes nos respectivos *hosts* a inventariar.

- × O OCS, contudo, não permite que se crie um novo registo de um equipamento que não suporte o protocolo SNMP ou no qual não seja possível configurar um agente, como por exemplo: ecrãs de computador, ratos e colunas de som, entre outros.

Escolha das Ferramentas

No geral, as ferramentas mencionadas anteriormente mostraram-se ser capazes de atingir (no geral) os objectivos pretendidos para monitorizar e gerir a rede do CCCEE, divergindo simplesmente no método de actuação para alcançar esses mesmos objectivos.

Embora o Cacti tenha uma comunidade de utilizadores activa, devido ao facto de trabalhar com base na adição de *plugins* para poder implementar diferentes funcionalidades –, esta ferramenta foi excluída por sujeitar os gestores da rede a depender, directa e/ou indiretamente, de outros "desenvolvedores", para manter os *plugins* constantemente actualizados e compatíveis com o Cacti.

O Icinga, contudo, apresentou-se neste ponto mais independente em comparação ao Cacti, uma vez que a ausência da configuração de *plugins* na aplicação não diminuiu a capacidade da ferramenta para apoiar a gestão e monitorização da rede. No entanto, o seu principal ponto negativo e que levou à exclusão da ferramenta assenta no facto de obrigar que qualquer configuração seja realizada através da linha de comandos em ficheiros de texto, tornando o processo de definição dos equipamentos uma tarefa mais lenta, em comparação com o Cacti e com o Zabbix. Existem, consequentemente, também maior probabilidade de ocorrerem erros na escrita do código nos ficheiros, invalidando assim o ficheiro e a veracidade dos dados monitorizados dos equipamentos. Embora a documentação do Icinga disponibilize algumas técnicas para optimizar este processo, as mesmas podem não ter grande impacto numa situação que englobe um grande número de equipamentos.

O Zabbix, em comparação com o Cacti e com o Icinga, fornece um pacote de funções de raiz mais completo, sem que exija portanto a necessidade de recorrer à utilização de *plugins.* E, apesar do Zabbix não detectar a ocorrência de *flapping* automaticamante*,* este disponibiliza a definição de alertas inteligentes ('*hysteresis*') que ajudam a resolver a situação de *flapping*; o Zabbix não destacou nenhum outro ponto fraco significativo em relação às outras funcionalidades.

Relativamente à área de gestão de inventários, embora tanto o Cacti como o Icinga e o Zabbix disponibilizem esta funcionalidade, o OCS Inventory NG foi a ferramenta que se destacou no registo dos equipamentos do CCCEE, para armazenar e visualizar os dados de

hardware e *software* dos vários equipamentos. Revelando-se uma solução prática e intuitiva de configurar.

Em suma, como soluções finais surge a ferramenta **Zabbix**, para monitorizar e gerir a rede e os sistemas do campus informático do CCCEE, e a ferramenta **OCS Inventory NG**, para manter um registo actualizado dos componentes de *software* e de *hardware* do CCCEE.

Na secção 4.3 apresenta-se a arquitectura da solução para o problema na área de gestão de redes do CCCEE.

4.3. Arquitectura da Solução

A abordagem às ferramentas integradas direcionadas para a área de gestão e monitorização de redes e sistemas, para o cenário do CCCEE, deveu-se ao facto de estas disponibilizarem, num único pacote, várias funcionalidades que "permitem resolver" vários problemas de diferentes áreas da gestão. Desta forma, não é necessário configurar uma ferramenta para cada tipo de problema. A adopção desta opção possibilita, desta forma, minimizar a questão de falta de recursos (financeiros e humanos) direcionados especificamente para a gestão e monitorização da rede e dos sistemas do CCCEE.

Através do levantamento dos problemas e das necessidades relacionadas com o sistema informático do CCCEE, foi possível identificar-se as principais áreas funcionais do modelo FCAPS a focar no cenário do CCCEE: a gestão de falhas, gestão de configuração e gestão de desempenho. Contudo, por não se tratarem de funcionalidades estanques, as áreas de gestão de contabilização e gestão de segurança serão também parcialmente cobertas.

O tipo de abordagem e o grau de abrangência às cinco áreas funcionais dependem directa e indirectamente das ferramentas implementadas (Zabbix e OCS Inventory NG) que, embora juntas integrem um conjunto variado de funcionalidades, não cumprem ao detalhe com todas as subfuncionalidades do modelo FCAPS (ver Tabela 1), em particular a da área de gestão de segurança.

Como se pode observar na Figura 11, à ferramenta Zabbix foi atribuída a tarefa da gestão e monitorização dos computadores, servidores, serviços, impressoras e outros equipamentos e recursos da rede informática sob responsabilidade do CCCEE, actuando particularmente nas áreas de gestão de falhas e de desempenho. Por sua vez, o OCS Inventory NG, ficou responsável pela função de inventário de todos os sistemas mencionados anteriormente, incluindo ainda o registo dos componentes de *software* e suas respectivas licenças, cobrindo parcialmente a área funcional de Gestão de Configuração.

A implementação eficiente de um modelo de gestão das TI numa organização é, cada vez mais, um factor quase (se não mesmo) imprescindível para auxiliar as tomadas de decisões dos administradores no processo de gestão de uma infra-estrutura informática. Deste modo, através de uma análise aos diferentes estados do ciclo de vida de um serviço, pelo Modelo ITIL – descrito na secção 2.3 –, identificou-se o estado **Operação de Serviço** (*Service Operation*) [26] como o principal estado a focar neste trabalho.

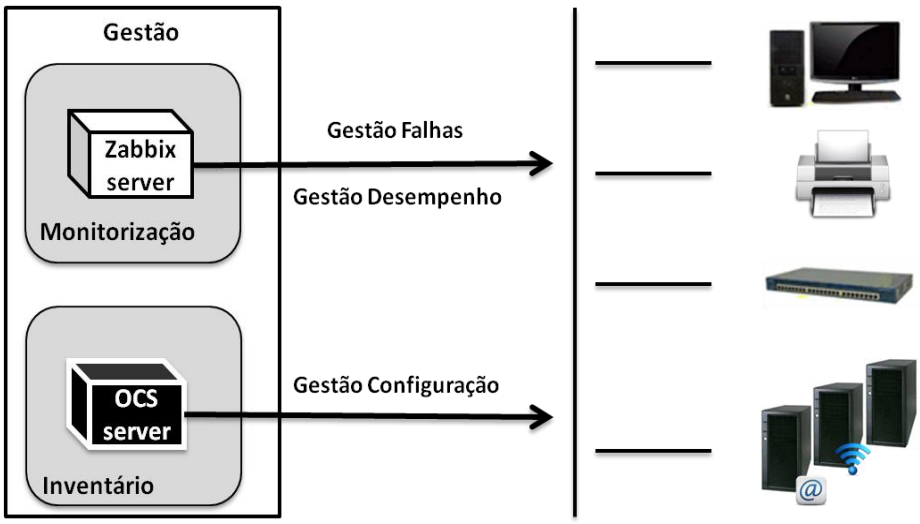


Figura 11 – Ferramentas e áreas funcionais de gestão de redes abrangidas

Assim, aplicando os três principais processos disponibilizados pelo estado **Operação de Serviço**, o administrador do CCCEE tem um conjunto de orientações sobre como deve actuar para alcançar a eficácia e a eficiência na entrega e suporte de serviços, de modo a assegurar o valor dos mesmos para os utilizadores e para o CCCEE.

- O fluxo de processos da **Gestão de Eventos** (ver Anexo A) tem como objectivo dar ao administrador a capacidade de detectar eventos, entendê-los e determinar a acção adequada de resposta aos mesmos. Segundo o ITIL, **'Eventos'** podem ser definidos como "qualquer ocorrência detectável ou perceptível que tem importância para a gestão da infra-estrutura de TI ou para a entrega de serviços de TI, e a avaliação do impacto que um desvio pode causar aos serviços" [26].

- Por sua vez, o fluxo de processos da **Gestão de Incidentes** (ver Anexo B) guia o administrador nas tarefas para restaurar o funcionamento normal dos serviços o mais rápido possível e minimizar o impacto negativo, de forma a garantir assim que os melhores níveis possíveis de qualidade são mantidos. Na terminologia do ITIL, um **'Incidente'** é definido como "uma interrupção não planeada de um serviço de TI ou a redução da qualidade de um serviço de TI. A falha de um item de configuração que ainda não teve impacto no serviço, também é um incidente" [26].

- Por último, o fluxo de processos da **Gestão de Problemas** (ver Anexo C) disponibiliza ao administrador a estratégia para evitar que os problemas e incidentes aconteçam, eliminar incidentes recorrentes e minimizar o impacto dos incidentes que não podem ser evitados. O ITIL define um **'Problema'** como "a causa para um ou mais incidentes" [26].

Um outro conceito, também importante para este trabalho, trata-se do conceito de **'Alerta'**. Pela terminologia do Modelo ITIL, o propósito de um alerta é garantir que, sempre que um evento obrigue à intervenção de uma pessoa, a pessoa com as capacidades apropriadas para lidar com esse evento seja notificada.

Para o processo de gestão e monitorização dos sistemas do CCCEE, após uma análise aos vários tipos equipamentos e sistemas presentes no campus informático do CCCEE, considerou-se apenas necessária a criação de quatro grupos, apresentados na Tabela 6, para organizar as diferentes máquinas.

Tabela 6 - Grupos de máquinas

Computadores	Servidores	Máquinas Virtuais	Outros Dispositivos
• SO *Windows* • SO *Linux* • SO Mac OS	• Servidores *Web* • Servidores Base de Dados • Servidores *E-mail* • Servidores *Backup*	• *VMware* • *VirtualBox* • *Hypervisors* (*Virtual Machines Monitor*)	• Impressoras • *Swicthes* • *Routers* • UPS

Na implementação das duas ferramentas, a solução adoptada para o cenário do CCCEE – e apresentada na Figura 12 – baseia-se numa arquitectura centralizada, utilizando-se uma topologia funcional do tipo gestor-agente, abordada pelas arquitecturas de gestão OSI e TMN, mas principalmente pelo SNMP das redes TCP/IP, descritas no Capítulo 2 do Estado da Arte.

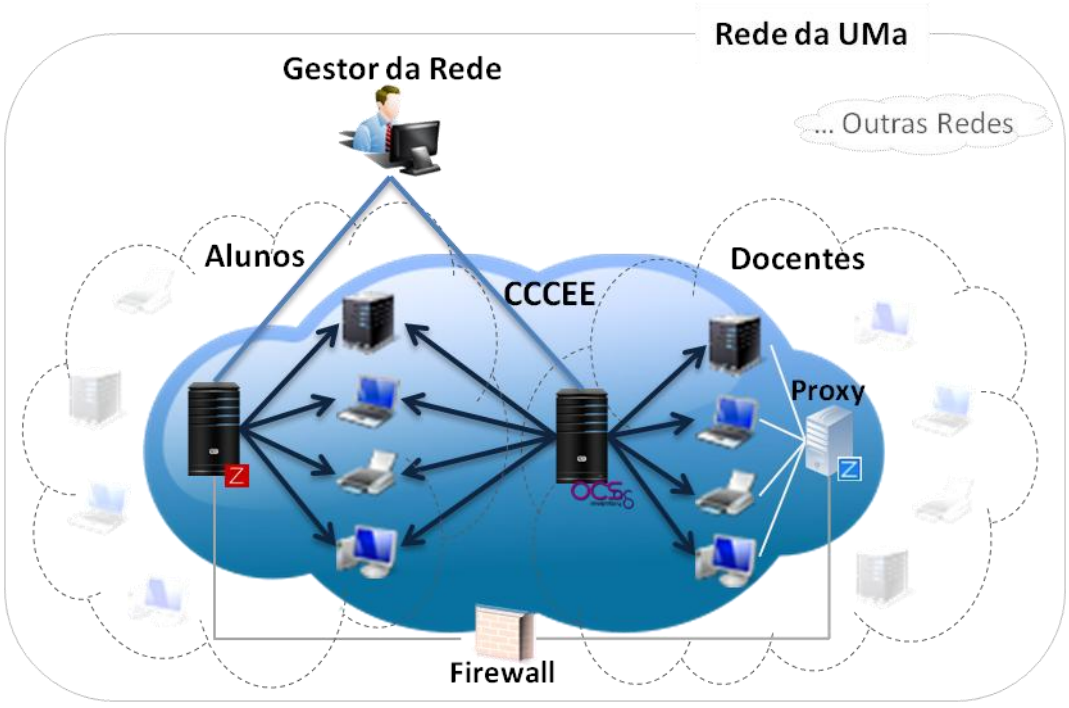


Figura 12 - Arquitectura Geral da Solução na Rede do CCCEE

Nesta arquitectura, a entidade gestora do Zabbix (*Zabbix Server)* encontra-se a funcionar na rede dos alunos, não tendo permissão para atuar sobre os sistemas da rede dos docentes; ao contrário do que acontece com a entidade gestora do OCS (*OCS Management Server)*. De modo a contornar este problema, uma possível solução passaria por implementar o *proxy* do Zabbix na rede dos docentes, sendo apenas necessário configurar a ligação entre o proxy e o servidor do Zabbix, para que as duas entidades possam se comunicar.

Para a criação das condições básicas ao estabelecimento da comunicação entre os sistemas a gerir e entre as entidades gestoras de ambas as ferramentas, procedeu-se às seguintes tarefas: habilitação do serviço SNMP (ver Anexo D e Anexo E) nos vários equipamentos na rede; à configuração dos agentes (ver Anexo F e Anexo G) disponibilizados por ambas as ferramentas de gestão; e, ainda, à definição de algumas regras nas *firewalls*. Embora a utilização de agentes obrigue a despender algum tempo na configuração dos mesmos nos vários equipamentos do CCCEE, essa desvantagem é compensada por se conseguir obter um maior número de dados monitorizados e com um maior detalhe.

É de referir, ainda, que, a aplicação de gestão Zabbix consegue analisar qualquer sistema independentemente do serviço de DHCP com que o mesmo esteja a funcionar. Contudo, por ter-se encontrado problemas no funcionamento do serviço de DNS na rede do CCCEE – que impossibilitavam a tradução dos IP's dinâmicos das máquinas para os seus respectivos nomes de domínio –, a tarefa de monitorização, durante a fase de testes – que será descrita no Capítulo 5 –, direcionou-se somente para os sistemas configurados com IP estático.

Na prática, a monitorização dos sistemas e da rede informática irá consistir na observação periódica dos equipamentos e serviços geridos, através da qual os administradores da rede conseguirão adquirir mais conhecimento acerca do estado da rede podendo actuar de modo mais eficiente sobre a mesma. Por sua vez, a gestão da rede fica direcionada não só ao controlo e à monitorização da utilização dos recursos da rede e sistema informático, como também à gestão de todos os sistemas através de um inventário.

Na secção seguinte, prossegue-se com a apresentação do processo de configuração de gestão e monitorização da infra-estrutura informática do CCCEE.

4.3.1. Gestão e Monitorização da Rede

Numa rede com a dimensão do CCCEE, que integra algumas centenas de sistemas a funcionar, tornar-se-ia inviável configurar individualmente os parâmetros de monitorização para cada um dos equipamentos da rede. Assim, de modo a optimizar todo esse processo de configuração, recorreu-se à utilização de *Templates* que possibilitam afectar vários *hosts* em simultâneo, ou seja, sempre que for realizada uma alteração a nível do *Template*, essa alteração propagar-se-á a todos os *hosts* a ele ligados.

Um T*emplate* pode, então, ser definido como um modelo que integra um conjunto de entidades (ou regras) de monitorização, que podem ser aplicadas a vários sistemas e equipamentos, não sendo por isso necessário configurar várias vezes a mesma regra para os diversos *hosts* a monitorizar.

Pode-se associar um ou mais *Templates* a um mesmo *host*, em que todas as entidades serão herdadas dos *Templates* vinculados. No Zabbix, cada *Template* abrange a definição de todas (ou algumas) das seguintes entidades [48]:

- ***Items*** – Representa uma métrica individual, que pode ser entendida como um identificador ou tipo de dados, que define exactamente o parâmetro que se pretende medir e monitorizar num *host*;
- ***Applications –*** Permite organizar os *items* monitorizados em grupos lógicos;
- ***Triggers*** – Expressão lógica que define um limite do que pode ser um problema, avaliando quando é que uma situação merece atenção. Um *trigger* é lançado quando a informação de um *item* corresponde a uma condição de problema;
- ***Screens*** – Trata-se de uma tabela que pode ser personalizada para permitir a visualização rápida da informação de várias fontes. A informação apresentada pode referir-se a: gráficos, mapas, texto simples, estado do sistema, entre outros;
- ***Graphs*** – Representa, através de gráficos, os valores dos dados obtidos pelos *items*, possibilitando uma melhor visualização do desempenho e comportamento da rede;
- ***Discovery rules*** – Permite iniciar a monitorização, por exemplo, dos sistemas de arquivos ou das várias interfaces de rede, sem a necessidade de criar um *item* para cada sistema de arquivo ou interface;
- ***Web scenarios*** – Consiste numa ou mais solicitações http para verificar a disponibilidade de uma página *web.*

Existem vários tipos de *items* disponibilizados pela ferramentas, entre os quais: agente Zabbix, SNMP, IPMI, JMX e *agentless monitoring* (ICMP, SSH e Telnet); em que se deve especificar que tipos de dados (*item key*) devem ser recolhidos dos *hosts* a monitorizar, para que os mesmos sejam analisados.

Para cada um dos grupos de máquinas definidos na secção 4.3, monitorizaram-se diferentes tipos de dados, para que fornecessem a informação acerca da disponibilidade e do funcionamento das várias máquinas da rede. As tabelas presentes nesta subsecção foram construídas com base nas informações adquiridas através da exploração/utilização da ferramenta.

No grupo dos 'Computadores' e 'Servidores', monitorizou-se os dados referentes ao processador, disco e memória, identificados no levantamento de requisitos realizados na secção 3.3.1 e, ainda, um conjunto de outras informações, apresentadas na Tabela 7, para os sistemas operativos *Windows* e *Linux*.

Tabela 7 - Dados monitorizados nos servidores *Windows* e *Linux*

	Windows	***Linux***
CPU	*Processor Load*	*Processor Load*
	CPU usage	*CPU idle time*
		CPU interrupt time
		CPU iowait time
		CPU nice time
		CPU softirq time
		CPU steal time
		CPU system time
		CPU user time
		Interrupts per second
		Context switches per second
Disk	*Allocation units for storage*	*Allocation units for storage*
	Description of storage	*Descriptio of storage*
	Total disk space	*Total disk space*
	Used disk space	*Used disk space*
File Systems	*Average disk read quele length*	*Free disk space*
	Average disk write quele length	*Free inods*
	File read bytes per second	*Total disk space*
	File write bytes per second	*Used disk space*
	Free disk space	
	Total disk space	
	Used disk space	
General	*Device contact details*	*Device contact details*
	Device description	*Device description*
	Device location	*Device location*
	Device uptime	*Device uptime*
	Number of threads	*Host boot time*
	Number of processes	*Host local time*
	Processe status	*Maximum number of opened files*
		Maximum number of processes
		Processe status
Security		*Checksum of /etc/passwd*
		Number of logged in users
Memory	*Free swap space*	*Free swap space*
	Total swap space	*TYotal swap space*
	Free memory	*Total memory*
		Available memory
Interfaces	*Admin status of interface*	*Admin status of interface*
	Alias of interface	*Alias of interface*
	Description of interface	*Description of interface*
	Inbound errors of interface	*Inbound errors of interface*
	Incoming traffic on interface	*Incoming traffic on interface*
	Operational status of interface	*Operational status of interface*
	Outbound errors of interface	*Outbound errors of interface*
	Outgoing traffic on interface	*Outgoing traffic on interface*
	Incoming network traffic on interface	*Incoming network traffic on interface*
	Outgoing network traffic on interface	*Outgoing network traffic on interface*
Services	*Services state (dhcp, htp, ssh,…)*	*Services state (dhcp, htp, ssh,…)*

Outro tipo de sistemas que também é possível monitorizar com o Zabbix são as máquinas virtuais e os *hypervisors*[4]. Contudo, pelo Zabbix, pode se consider uma máquina virtual como uma máquina real, aplicando-se às VM os mesmos Templates que para uma máquina real.

[4] ***Hypervisors*** – Também conhecido como V*irtual Machine Manager* (VMM), é um programa de *software* que permite que vários sistemas operacionais partilhem um único host. É quem controla o processador, memória e outros recursos, alocando o que cada SO necessita.

Por sua vez, para os hypervisors pode-se conhecer um conjunto de parâmetros específicos como os apresentados na Tabela 8.

Tabela 8 - Dados monitorizados num *Hypervisor*

	Hypervisor
General	*Full name*
	Version
	Uptime
	Hypervisor name
	Power state
	Overall status
	Number of guest VM
	Cluster Name
Log	*Event Log*
Hardware	*Number of virtual CPU's*
	CPU cores
	CPU frequency
	CPU model
	CPU threads
	CPU usage
	Bios UUID
	Model
	Vendor
	Total Memory
Storage	*Commited storage space*
	Uncommited storage space
	Unshared storage space
Memory	*Memory size*
	Available memory
	Host memory usage
	Guest memory usage
	Swapped memory
	Shared memory
	Private memory
	Compreddes memory
	Balloned memory
Disk	*Average number of kilobytes read from the disk*
	Average number of kilobytes written to the disk
Filesystems	*Free disk space*
	Total disk space
	Used disk space
Interfaces	*Number of bytes received on interface*
	Number of bytes transmitted on interface
	Number of packets received on interface
	Number of packets transmitted on interface
	Incoming network traffic on interface
	Outgoing network traffic on interface
Services	*Services state (dhcp, htp, ssh,…)*

Nos servidores de armazenamento de dados, a operar apenas com o sistema operativo *Linux*, monitorizou-se ainda os dados correspondentes ao sistema de gestão de base de dados MySQL, apresentados na Tabela 9.

Tabela 9 - Dados Monitorizados no MySQL

Linux	
MySQL	MySQL *begin operation per second*
	MySQL *bytes received per second*
	MySQL *bytes sent per second*
	MySQL *commit operations per second*
	MySQL *delete operations per second*
	MySQL *Insert operations per second*
	MySQL *queries per second*
	MySQL *rollback per second*
	MySQL *select per second*
	MySQL *slow queries*
	MySQL *status*
	MySQL *update operations per second*
	MySQL *uptime*
	MySQL *version*

No grupo dos 'Outros Dispositivos', por exemplo das impressoras, monitorizou-se o nível dos tinteiros e a quantidade de papel, sendo que a ferramenta possibilita ainda obter dados sobre o estado das interfaces, a descrição da impressora, entre outras informações como as apresentadas na Tabela 10.

Tabela 10 - Dados monitorizados numa impressora

Impressoras	
General	*Device description*
	Device name
	Device uptime
Supplies	*Supplies description*
	Max capacity
	Cartridge level
Other	*Life count*
	Photo conductor units
	Power on count
	Storage size
	Storage used
Interfaces	*Admin status of interface*
	Description of interface
	Inbound errors on interface
	Incoming traffic on interface
	Operational status of interface
	Outbound errors on interface
	Outgoing traffic on interface

Embora não tenham existido as condições para se monitorizar os *swicthes*, *routers* e UPS (*Uninterruptible Power Supply*) do CCCEE, a ferramenta encontra-se também preparada para monitorizar estes últimos dispositivos.

Embora se possam monitorizar outros parâmetros de interesse, os parâmetros mais frequentes a monitorizar nos *switches* e *routers*, incluem essencialmente:

- O Estado das Interfaces;
- O Fluxo de Dados das Interfaces;
- A Carga do Processador;
- A Carga de Memória;

No caso da monitorização das UPS, recomenda-se, no mínimo, a monitorização das seguintes variáveis:

- Estado da UPS (modo de bateria, modo *online*, mau funcionamento);
- Capacidade da bateria;
- Temperatura da bateria;
- Carga de saída da UPS;
- Tensão de entrada/saída, e;
- *Input* /*Output* Actual.

Para adquirir e analisar informações importantes de *hardware* relativas aos diferentes tipos de sensores de diferentes equipamentos – temperaturas, velocidades da ventoinha (*fan speed),* voltagem *do sistema (system voltages),* estado físico do disco *(state of the physical disk)* e estado de manutenção (*maintenance LED status)* –, é necessário que os sistemas a monitorizar contenham uma interface IPMI configurada.

Por sua vez, se existir a necessidade de monitorizar funções que são específicas de um determinado vendedor, deve-se pesquisar e analisar as MIB do vendedor que fabricou o respectivo dispositivo.

A funcionalidade *Web Monitoring*, da aplicação Zabbix, possibilita recolher indicadores sobre uma página web. Esta funcionalidade não se trata de uma monitorização de um servidor web, mas sim da monitorização da página da organização ou da página intranet, por exemplo, da página do Moodle. No *Web Monitoring,* existem dois tipos de monitorização: a simples, que apenas verifica se a página está disponível *online*, e a complexa, em que se pode verificar, por exemplo, se os utilizadores estão a conseguir fazer *login*.

Na monitorização complexa definem-se '*web scenarios*' que consistem em uma ou mais etapas, ou pedidos de http. Estes pedidos são executados periodicamente pelo *Zabbix Server,* pela ordem pré-definida na configuração. Através desta funcionalidade, consegue-se adquirir a seguinte informação referente à monitorização de uma página web:

- Velocidade média de *download,* por segundo, durante todas as etapas;
- Número da etapa que falhou;
- Última mensagem de erro;
- Velocidade de *download* da página, por segundo;
- Tempo de resposta, e;
- Código http de resposta.

Assim que os dados dos sistemas monitorizados são adquiridos na aplicação, através dos diferentes métodos de recolha de informação, o processo de detecção, avaliação e notificação de eventos inicia-se.

Um aspecto importante no processo de resposta a um evento é atribuir um nível de importância adequado a um problema, de forma a determinar como um evento deverá ser tratado quer pela ferramenta de gestão e monitorização como também pelos gestores da rede. Normalmente, diferenciar a importância de um problema pode ser determinado tendo em conta a urgência do problema (a rapidez com que o CCCEE precisa de uma resolução) e o

nível de impacto que poderá originar. Uma indicação do impacto poderá ser, por exemplo, o número de utilizadores que serão afetados pelo respectivo problema.

O Zabbix possibilita atribuir a um problema um de entre seis níveis de gravidade, que permitem distinguir o grau de importância de um problema, como apresentado na Figura 13.

Figura 13 - Níveis de gravidade de um problema

O mecanismo utilizado para iniciar o processo de resposta a um evento denomina-se por *trigger*. A tarefa de um *trigger* é o de avaliar e comparar os dados obtidos pelos *items* com o valor definido pelo administrador, que determina quando uma situação deve ser considerada um problema. Ou seja, a ideia subjacente a um sistema de *triggers* é desencadear alertas sempre que um valor limite (mínimo ou máximo) é atingido, mantendo um registo da ocorrência desse evento e enviando uma notificação ao administrador da rede, para que este último possa agir de acordo com o evento gerado.

Um *trigger* é accionado, por exemplo, quando um serviço ou uma máquina muda o seu estado com muita frequência. A este tipo de situações denomina-se por *flapping*. Da ocorrência de *flapping* resultam: 1) um bombardeamento de notificações enviadas aos administradores de redes a reportar o problema, e 2) a sua respectiva recuperação.

O sistema de *triggers* fornecido pelo Zabbix permite utilizar vários *items* obtidos de diferentes fontes para se definir uma expressão lógica mais complexa e inteligente (‘*hysteresis’)*, de forma a minimizar a notificação de *flapping* e, ainda, estabelecer dependências entre *triggers* para evitar alertas sobre falsos positivos. Uma regra simples de um *trigger* pode ser criada utilizando a seguinte expressão:

- { <*server*> : <*key*> . <*function*> (<*parameter*>) } <*operator*> <*constant*>

Na prática, para avaliar se o espaço livre do Disco ‘C:’, do servidor do CCCEE ‘*ceesoftkeys’,* é (ou não) inferior a 10%, a expressão anterior ficaria definida da seguinte forma:

- *{ ceesoftkey : vsf.fs.size [C: , pfree] . last (0) } < 10*

Assim, se o último valor retornado <*last(0)*> pela expressão *{ceesoftkey : vsf.fs.size [C: , pfree]}* for inferior a 10, a regra torna-se verdadeira e o *trigger* é acionado.

Organização do Sistema de Gestão de Alertas

Apesar de actualmente os recursos humanos responsáveis pela gestão serem escassos no CCCEE, em redes de média e grande dimensão, o ideal seria que as tarefas de gestão e monitorização da rede e dos sistemas fossem distribuídas por vários técnicos. Esses técnicos seriam organizados por diversos grupos que ficariam responsáveis por actuar em diferentes problemas. Deste modo, de entre os grupos sugeridos na própria aplicação do Zabbix e da análise aos problemas e dimensão do CCCEE, propôs-se a criação de sete grupos de gestores, apresentados no esquema da Tabela 11.

Tabela 11 – Proposta de organização das tarefas de gestão e monitorização

Help Desk	• Primeira equipa a intervir quando os utilizadores da rede notificam algum incidente. Estes incidentes podem incluir desde: erros de rede, *hardware* e *software* (por ex: dificuldades em executar determinadas operações), como ainda pedidos de serviços (por ex: renovação ou emissão de novas passwords);
Windows Admin	• Equipa responsável por atuar sobre os sistemas sob o SO Windows;
Linux Admin	• Equipa responsável por actuar sobre os sistemas sob o SO Linux;
Database Admin	• Equipa que intervem nos problemas ocorridos nos sistemas de base de dados;
Security Especialist	• Equipa responsável pela área da gestão de segurança;
IT Management	• Equipa que mantém o primeiro contacto com os problemas da rede e dos serviços;
Network Admin	• Equipa responsável por assegurar e manter a gestão e monitorização de toda a infra-estrutura informática, actuando nos problemas mais críticos;

Contudo, na prática, por só existirem dois gestores na rede do CCCEE, as tarefas descritas para cada grupo no esquema da Tabela 11, têm de ser partilhadas pelo administrador e pelo técnico do CCCEE. Assim, o sistema de gestão de alertas da ferramenta de gestão foi configurado de modo mais simples, tendo-se passado dos sete grupos definidos no esquema anterior para apenas quatro grandes grupos (Rede, Serviços, *Hardware* e *Software*), segundo a arquitectura apresentada na Figura 14.

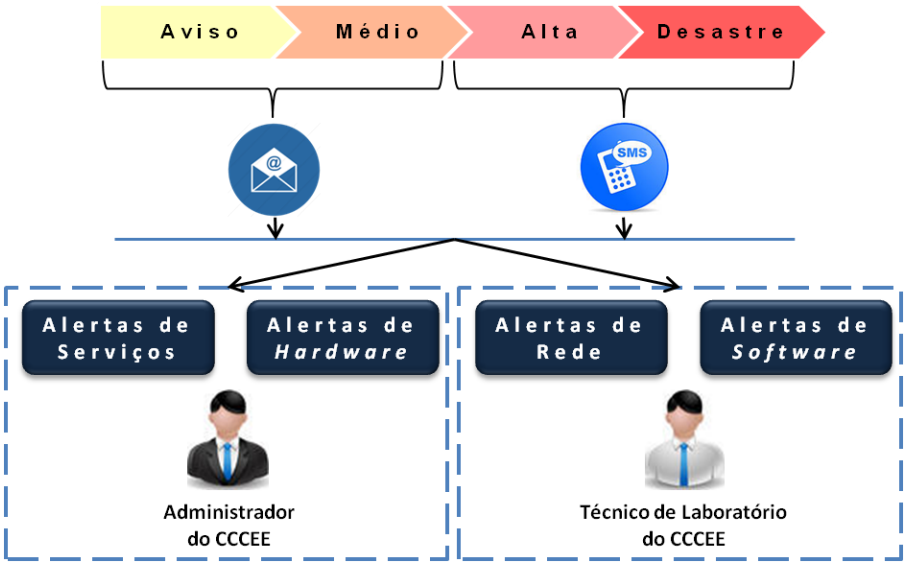


Figura 14 - Arquitectura do Sistema de Gestão de Alertas

Nesta arquitectura utilizam-se apenas quatro níveis de gravidade para classificar um problema, menos dois que na Figura 13, sendo que o tipo de notificação enviada aos gestores do CCCEE (via e-mail ou via sms), fica dependente do nível de gravidade utilizado para classificar os problemas detectados. A ocorrência de problemas classificados como "Sem classificação" e "Informação" ficam apenas registados na aplicação. O administrador do CCCEE fica então responsável por actuar nos alertas dos Serviços e de *Hardware*, e o técnico a cargo do grupo de alertas da Rede e de *Software*. De referir que, até à data da escrita deste documento, todos os grupos de alertas se encontravam configurados para serem enviados aos gestores do CCCEE apenas via *e-mail*.

Para a infra-estrutura informática do CCCEE, configuraram-se *triggers* para avaliar a disponibilidade de todos os sistemas monitorizados pela aplicação, tendo-se ainda utilizado os valores dos *triggers* fornecidos pela aplicação para avaliar os outros componentes monitorizados. Por exemplo, são enviados alertas quando ocorrem os seguintes *triggers*:

- **Espaço e utilização do disco** – quando o espaço livre do disco se aproxima dos 20% e/ou, quando o número de pedidos ao disco aumentam significativamente pode afectar o desempenho do sistema tornando-o mais lento;
- **Carga e utilização do processador** – quando a utilização ou a carga do processador se mantêm em valores superiores a 85%, o sistema pode parar de responder e/ou sobreaquecer o CPU;
- **Quantidade de memória** – quando o consumo excessivo de memória ultrapassar os 80% poderá influenciar, por exemplo, a velocidade de desempenho do sistema;
- **Tráfego in/out –** quando existe um consumo elevado de tráfego de rede;
- **Estado dos serviços** – um serviço parado poderá afetar determinadas aplicações ou *softwares* que dependam do mesmo para funcionar normalmente;
- **Número de processos** – se o sistema está com 30 processos abertos, o CPU pode ficar sobrecarregado;
- **Modificação de valores em ficheiros –** quando o valor de um ficheiro crítico como, por exemplo, o ficheiro /etc/passwd (que guarda informação dos utilizadores), é alterado ou modificado;
- **Agente de monitorização inacessível** – quando o agente não se encontra a recolher dados ou está inacessível significa que parte da informação dos sistemas não se encontra a ser monitorizada pelo sistema de gestão, e;
- **Estado das impressoras** – quando o nível de tinta é inferior a 10%, é um indicador que o tinteiro deve ser substituído.

De forma a ser possível obter uma visão geral da infra-estrutura da rede informática do CCCEE, pode ser utilizada a funcionalidade de criação de mapas de rede, exemplificado na Figura 15. Cada *icon* adicionado ao mapa pode representar um único sistema, um grupo de sistemas, um simples alerta, uma imagem ou mesmo um outro mapa. Pode-se definir as informações que serão apresentadas com esses mesmos *icons* e, ainda, que dados deverão ser apresentados nas ligações entre os *icons*.

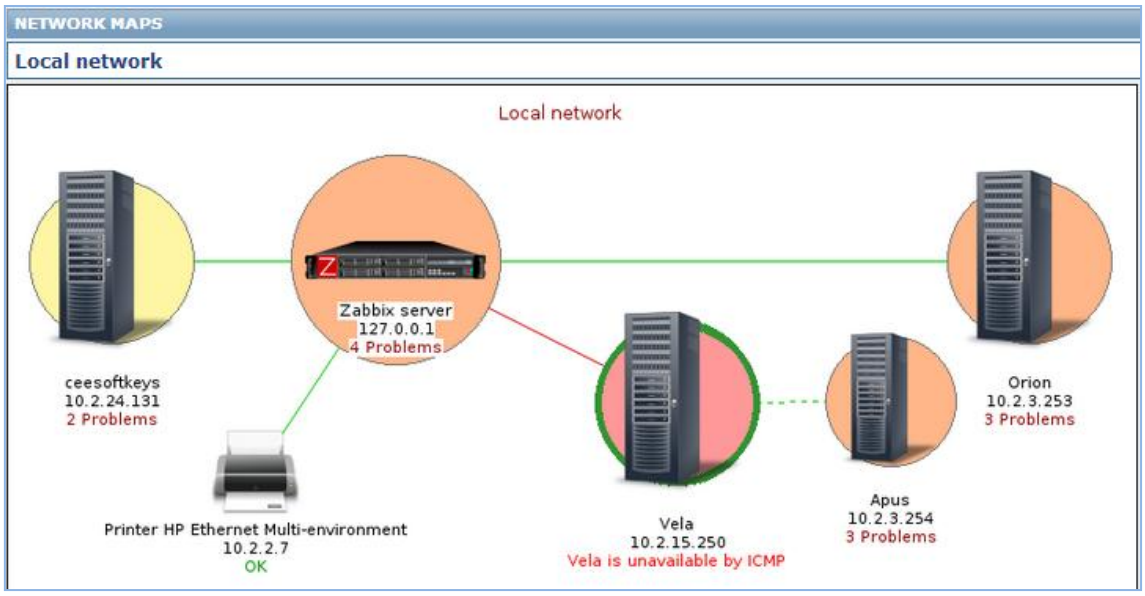


Figura 15 – Mapa da Rede

É, ainda, possível garantir a segurança na gestão da rede do CCCEE, permitindo ou restringindo o acesso de apenas alguns utilizadores a determinadas áreas, funções e sistemas monitorizados na aplicação.

Na secção seguinte, prossegue-se com a descrição da gestão do inventário dos componentes lógicos e físicos existentes no campus informático do CCCEE

4.3.2. Gestão de Inventário

Manter o inventário actualizado através do método tradicional do papel é uma tarefa que exige um grande esforço e mão-de-obra dedicada, principalmente para redes de média e grande dimensão. Para tornar esta tarefa automatizada, simples e com pouca intervenção humana, configurou-se, na rede do CCCEE, a ferramenta OCS Inventory para a gestão do inventário.

O processo de gestão do inventário dos equipamentos das instalações do CCCEE passou, inicialmente, pela configuração dos agentes do OCS nos vários equipamentos das instalações do CCCEE, sendo disponibilizados dois tipos de agentes:

- ***Local Inventory*** – Neste tipo de agente não é utilizado o acesso à rede. Ele gera e guarda o inventário no próprio equipamento em que é executado. O ficheiro criado com os dados do inventário deve ser salvo num dispositivo USB e, posteriormente, importado na aplicação OCS.

- ***Network Inventory*** – Neste tipo de agente é utilizado o acesso à rede. Ele envia, de modo automático, o inventário dos equipamentos ao *OCS Management Server*. O gestor tem a possibilidade de definir a frequência com o que os inventários devem ser actualizados.

O primeiro tipo de agente, '*Local Inventory*' foi direcionado para os equipamentos do CCCEE que não têm acesso à rede e, por essa razão, não têm a capacidade de alcançar o servidor OCS.

Por sua vez, configurou-se o '*Network inventory*' em todos os equipamentos existentes nas instalações do CCCEE, com condições de aceder à rede. Definiu-se, por padrão, a frequência de actualização dos inventários para ser executada sempre que o agente detectar qualquer alteração a nível do *hardware* e/ou *software* dos equipamentos.

No caso de máquinas que operam sob o SO *Windows*, direcionadas para as actividades de ensino ou de investigação do CCCEE, o agente '*Network inventory*' foi executado como um serviço do *Windows*, que se inicia automaticamente quando o computador é ligado.

No entanto, este tipo de agente pode também ser configurado localmente, i.e., sem correr como um serviço, sendo executado como um aplicativo independente, que pode ser inicializado através de um *script* de *login*, um GPO *Active Directory* ou, ainda, como um atalho no menu iniciar. Esta configuração – sem correr como um serviço – foi adoptada para os servidores do CCCEE, em que, embora o inventário continue a ser realizado de forma automática pelo agente, este último tem de ser executado manualmente pelo gestor da rede.

O agente '*Network inventory*' – para as máquinas *Windows* –, possibilita ainda escolher se os *softwares* existentes nos equipamentos devem ou não ser analisados. Esta última opção deve ser adoptada quando se pretender preservar a privacidade dos utilizadores, neste caso os professores e funcionários do CCCEE.

Nas máquinas que funcionam com o SO *Linux* implementado, o agente '*Network inventory*' pode apenas ser executado localmente, existindo contudo a opção de activar a actualização automática do mesmo, escolhendo o método de inventário http.

Como alternativa à utilização de agentes, pode-se utilizar os dois métodos fornecidos pela funcionalidade de descoberta automática na rede: '*IPdiscover'* e SNMP.

Ao contrário do que acontece com o registo dos equipamentos via SNMP, a função '*IPdiscover*' é limitada quanto à informação que fornece acerca dos dispositivos que detecta, sendo por essa razão mais vantajoso optar-se pelo inventário via SNMP. Contudo, o primeiro método fornece uma boa alternativa para registar, na aplicação, os sistemas que não suportem a configuração dos agentes OCS nem contenham o protocolo de comunicação SNMP habilitado.

Através da funcionalidade de descoberta automática, via SNMP, foi possível manter o inventário dos seguintes dispositivos de rede do CCCEE:

- Máquinas Virtuais
- Impressoras
- *Routers*
- *Switches*
- *Firewalls*
- UPS
- Computadores

Na Tabela 12 é apresentado um exemplo de um inventário obtido de uma impressora registada na aplicação OCS, através da funcionalidade de descoberta automática na rede, pelo método SNMP.

Tabela 12 - Dados obtidos de uma impressora registada na aplicação OCS, via SNMP

Tipo	Informação
Global informations	*IP address; SNMP device identification; Description; location; Type; CHECKSUM; MAC address; Name; Contact; Last come;Last inventory; Serial Number; Number, STATUS;*
Cartridges	*Type; Level; Maximum capacity; Color; Description; Percentage;*
Network (s)	*Description; MAC address; Status; MIB type; IP address;*
Trays	*Name; Description; Level; Maximum Capacity; Percentage;*
Processor (s)	*Manufacturer; Type; Frequency;*
Memory	*Capacity*;

No processo de inventário dos sistemas do campus informático do CCCEE, atribuiu-se ao valor da TAG a informação do tipo equipamento ou dispositivo a ser registado.

Pode-se, ainda, adicionar aos inventários dos equipamentos, informações que tanto o método SNMP como os agentes não têm a capacidade de adquirir. Essas informações abrangem, por exemplo, os seguintes parâmetros:

- **Responsável** – Gestor de rede responsável pela gestão do equipamento;
- **Estado de utilização** – Se um equipamento está em funcionamento ou fora de serviço;
- **Localização** – Piso da UMa, número da porta e nome do espaço;
- **Garantia** – Data de início e fim de garantia;
- **Licenças** – Data para a renovação e pagamento das licenças;
- **Informações Gerais** – Número de série, código, referência, assim como alguma senha importante dos equipamentos;
- **Notas** – Outras anotações/informações relevantes.

Os dados pertencentes aos inventários de qualquer sistema registado na aplicação OCS Inventory NG podem ser exportados para o formato XML.

Como mencionado na secção 2.4, onde se descreve a ferramenta OCS Inventory NG, pode-se definir dois tipos de grupos de equipamentos: estáticos, em que as máquinas são introduzidas e removidas de um determinado grupo apenas por acção do utilizador; e dinâmicos, onde a gestão dos grupos é executada pelo próprio *OCS Management Server*. Na Tabela 13 apresentam-se alguns dos diferentes grupos definidos para a organização dos diversos sistemas do CCCEE registados na aplicação.

Tabela 13 - Exemplos de grupos configurados na aplicação OCS

	Critérios	Nome do Grupo	Descrição
GRUPOD DINÂMICOS	Sistema Operativo	*Windows* *Linux*	Equipamentos a funcionar sob o sistema operativo *Windows*; Equipamentos a funcionar sob o sistema operativo *Linux*;
	Softwares	Wolfram Mathematica MathWorks MatLab	Equipamentos com o *software* Wolfram Mathematica; Equipamentos com o *software* MathWorks MatLab;
	Localização + *Software*	Nº porta X + Wolfram Mathematica	Equipamentos da sala de aulas na porta X, com o Wolfram Mathematica;
	Arquitecturas	x86 bits x64 bits	Computadores com processador de x86; Computadores com processador de x64;
	Tipo	*Desktop* *Servers* *VM* *Printers* *Switches*	Todos os computadores; Todos os Servidores Físicos; Todas as Máquinas Virtuais; Todas as impressoras; Todos os *Switches*;
	Rede	Docentes 10.1.0.0 Alunos 10.2.0.0	Máquinas na rede dos Docentes; Máquinas na rede dos Alunos;
	Localização	Nº porta X Pisos X	Máquinas que se encontram no espaço X; Máquinas existentes no piso X da UMa;
	Grupos de Utilizadores	Docentes Funcionários Alunos	Computadores utilizados pelos docentes; Computadores utilizados pelos funcionários do Centro; Computadores utilizados nas salas de aulas e laboratórios;
GRUPOS ESTÁTICOS	Servidores	Servidores *WEB* Servidor de Base de Dados	Todos os servidores *WEB*; Todos os servidores de base de dados;
	Licenças	Data X de Fim de Garantia Data X de Renovação	*Softwares* com data X de fim de garantia igual; *Softwares* com data X igual de renovação da licença;
	Gestor de Redes	Administrador CCCEE Técnico CCCEE	Máquinas sob a gestão do Administrador de Redes; Máquinas sob a gestão do técnico de laboratório;
	Estado	Manutenção	Todas as máquinas para (ou em) manutenção;

No geral, quer o administrador da rede quer o técnico de laboratório, têm acesso à totalidade das funcionalidades da ferramenta OCS, com a diferença que o primeiro é o único com permissão para gerir as contas de utilizadores que permitem o acesso à aplicação.

4.4. Conclusão

As tarefas de gestão e monitorização realizadas pelos administradores da rede do CCCEE, antes da implementação da solução implementada, eram realizadas pontualmente sobre um pequeno grupo de sistemas e limitadas apenas à análise de determinados recursos, como verificação do espaço de memória e do nível de carga do CPU.

Com a utilização da ferramenta Zabbix fica possível abranger um maior número de sistemas a gerir e aumentar também o conjunto de dados a monitorizar desses sistemas. Todos os dados adquiridos podem, ainda, ser organizados e visualizados através de gráficos, mapas e vistas (*screens*), que ajudam os gestores do CCCEE a analisar e a avaliar o estado dos sistemas da rede informática, sendo ainda alertados sobre a ocorrência de problemas.

As tarefas de gestão e monitorização da infra-estrutura informática do CCCEE tornam-se, desta forma, mais práticas e rápidas, uma vez que essas actividades deixam de ter que ser executadas individualmente de máquina a máquina, disponibilizando mais tempo para os gestores de rede do CCCEE poderem se dedicar a outras funções.

A ferramenta OCS Inventory NG permite, por sua vez, automatizar o processo de inventário mantendo, ao mesmo tempo, as informações dos inventários actualizadas. Adicionalmente, com a utilização das funcionalidades de pesquisa e criação de grupos, disponibilizadas pela ferramenta, torna-se mais simples para os gestores do CCCEE verificar, por exemplo, os *softwares* que um computador tem instalado e, ainda, o tipo e a quantidade de equipamentos que existem num determinado espaço de actividades de ensino e/ou de investigação.

Deste modo, numa primeira avaliação às ferramentas, pode-se afirmar que ambas conseguiram responder aos principais requisitos identificados no capítulo anterior.

5. Testes e Resultados

5.1. Introdução

O processo de implementação da solução passou previamente por várias etapas: desde o estudo das tradicionais arquitecturas de gestão de redes, à apresentação de modelos que auxiliam nas tomadas de decisões de gestão de TI, passando à análise das respectivas plataformas integradas, até ao levantamento da informação acerca da infra-estrutura informática e da definição dos seus problemas, assim como à fase de escolha das ferramentas até à implementação das mesmas na rede do CCCEE.

Neste capítulo apresentar-se-ão os resultados adquiridos após a implementação e testes realizados às ferramentas integradas na área de gestão e monitorização, tendo em conta os objectivos descritos no Capítulo 1.

Para a realização dos testes pretendia-se verificar a disponibilidade e o desempenho de todos os sistemas do CCCEE que estivessem integrados quer na rede dos docentes quer na rede dos alunos. No entanto, por não ter existido a possibilidade de gerir todos esses sistemas, o cenário utilizado para os testes abrangeu apenas um pequeno grupo de máquinas. Por conseguinte, as conclusões obtidas e apresentadas neste capítulo têm por base os resultados adquiridos dos testes efectuados ao pequeno grupo de máquinas. Assim, por ser uma prioridade para os administradores a monitorização e gestão dos servidores do CCCEE, o grupo de máquinas utilizado para os testes incluiu um conjunto de 5 servidores (4 sob SO *linux* e 1 sob SO *Windows*). Também se abrangeu uma impressora e cerca de 17 computadores (estes últimos utilizados principalmente para avaliar a solução de inventário).

Cada figura presente neste capítulo apresenta, na respectiva legenda, o intervalo de tempo da captura de informação dos dados monitorizados, considerando a seguinte nomenclatura: M-mês, d-dias, h-horas, m-minutos.

1. *Garantir uma gestão preventiva de todo o campus informático do CCCEE, de forma a prevenir ou evitar que uma situação fora do comportamento normal possa desencadear problemas;*

Mesmo os gestores de serviços e sistemas informáticos mais experientes, pouco ou nada podem fazer se não tiverem acesso às informações do que acontece a cada instante sobre a operacionalidade e funcionalidade da rede, para que consigam saber onde e como agir antecipadamente sobre as situações que se apresentam fora do comportamento normal.

Assim, a implementação do sistema de gestão e monitorização veio proporcionar aos gestores do CCCEE, a capacidade de agir de forma preventiva sobre os sistemas da rede informática, através de mecanismos que lhes permitem avaliar e identificar condições críticas que podem futuramente desencadear problemas ou falhas. Isto possibilitou que os gestores do CCCEE conseguissem agir atempadamente a um problema antes que o mesmo fosse sentido e notificado pelos utilizadores. O facto dos gestores da rede conseguirem acompanhar o funcionamento e o desempenho dos sistemas da infra-estrutura informática do CCCEE, também ajudou a que fossem identificadas mais facilmente situações como a subutilização ou sobreutilização de recursos da rede.

Um exemplo de subreutilização de recursos pode ser visualizado no gráfico da Figura 16, onde se pode observar que num determinado intervalo de tempo, de um conjunto de meses, ocorreu um pico de utilização do CPU no servidor Apus.

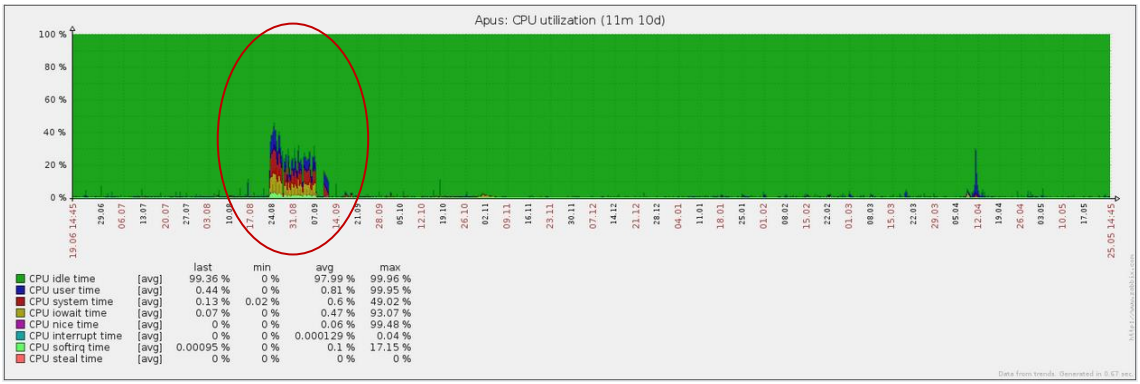


Figura 16 - Gráfico da Utilização do CPU no Servidor Apus (11M 10d) (a)

Numa análise mais detalhada à área assinalada com um círculo na figura anterior, que consta na Figura 17, pode-se verificar que o pico teve uma duração aproximada de 16 dias e que os valores de utilização do CPU estiveram acima do normal mas, em regra, abaixo dos 50%. Para esta situação e apesar do pico de utilização, considerou-se não ser necessário trocar de CPU, uma vez que os valores obtidos não prejudicaram o normal funcionamento do sistema.

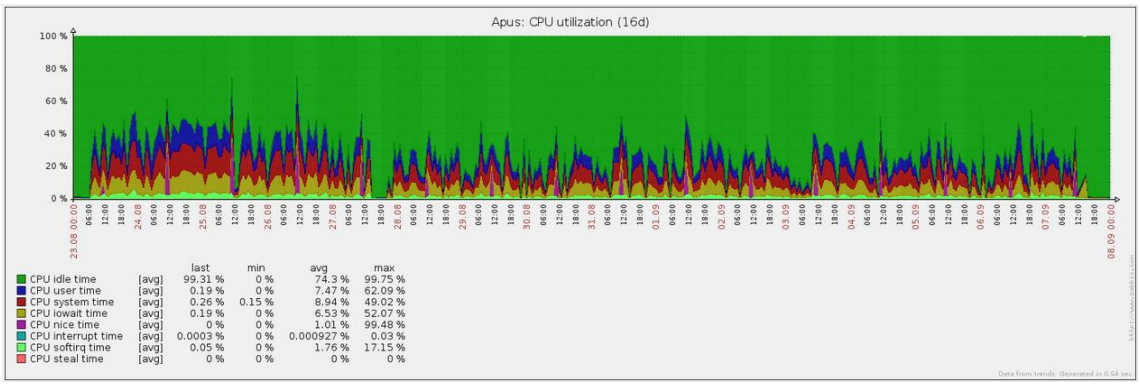


Figura 17 - Gráfico da Utilização do CPU no Servidor Apus (16d) (b)

No campus informático do CCCEE, existia uma máquina virtual com 2.5 GB de memória que foi substituída por uma máquina física com 4 GB, devido a uma avaria no *hardware* da primeira máquina. Após a troca de recursos entre as duas máquinas, o sistema de gestão e monitorização continuou a monitorizar e a registar as novas informações, situação que pode ser observada pela área assinalada com um círculo na Figura 18.

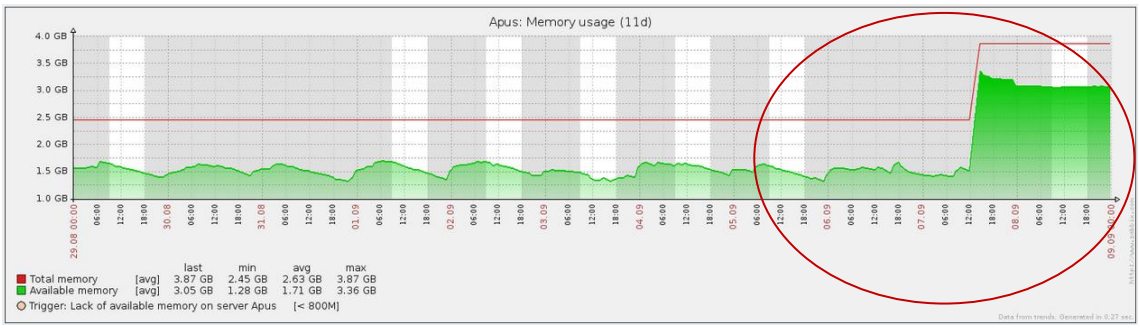


Figura 18 - Gráfico da Utilização da Memória do Servidor Apus (11d)

Relativamente à monitorização de páginas web, em particular a página do Moodle, a aplicação do Zabbix permite, por exemplo: acompanhar o redireccionamento de páginas, verificar a existência (ou não) de determinada *string* na página e verificar se um utilizador consegue fazer o *login.* Para além dos indicadores descritos anteriormente, ainda é possível calcular a informação da velocidade do carregamento da página, o tempo de resposta e o código do estado http recebido, como pode ser observado na Figura 19. O conjunto destes dados permite ao administrador saber se a página web está *online* e a funcionar normalmente.

DETAILS OF SCENARIO Moodle 14/15 Availability [30 Apr 2015 13:15:07]

Step	Speed	Response time	Response code	Status
Step 1 - Home	83.57 KBps	422.4ms	200	OK
Step 2 - Login	58.49 KBps	314ms	200	OK
TOTAL		**736.4ms**		**OK**

Figura 19 - Disponibilidade da página do Moodle

A visão global, ou vista (*screen*), possibilita uma visualização rápida dos dados monitorizados, através por exemplo de gráficos, mapas e/ou dados em texto. A informação disponibilizada numa vista pode fornecer apenas a informação de uma particularidade de um sistema do CCCEE ou integrar dados de múltiplos sistemas que podem ter (ou não) alguma semelhança. Por exemplo, pode-se construir uma visão global contendo apenas a informação do sistema de ficheiros de um único servidor do CCCEE, como pode ser observado na Figura 20. Ou, em alternativa, construir uma vista com vários sistemas (ceesoftkeys, Apus, Orion e Zabbix) com a informação de diferentes componentes como da carga do CPU e da quantidade de memória, como mostra a Figura 21.

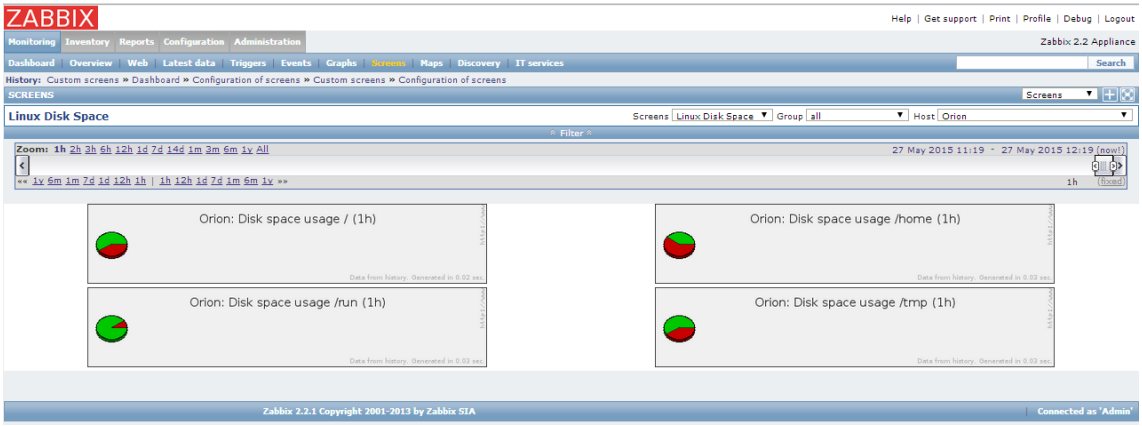


Figura 20 – Vista do estado do sistema de ficheiros do servidor Orion (1h)

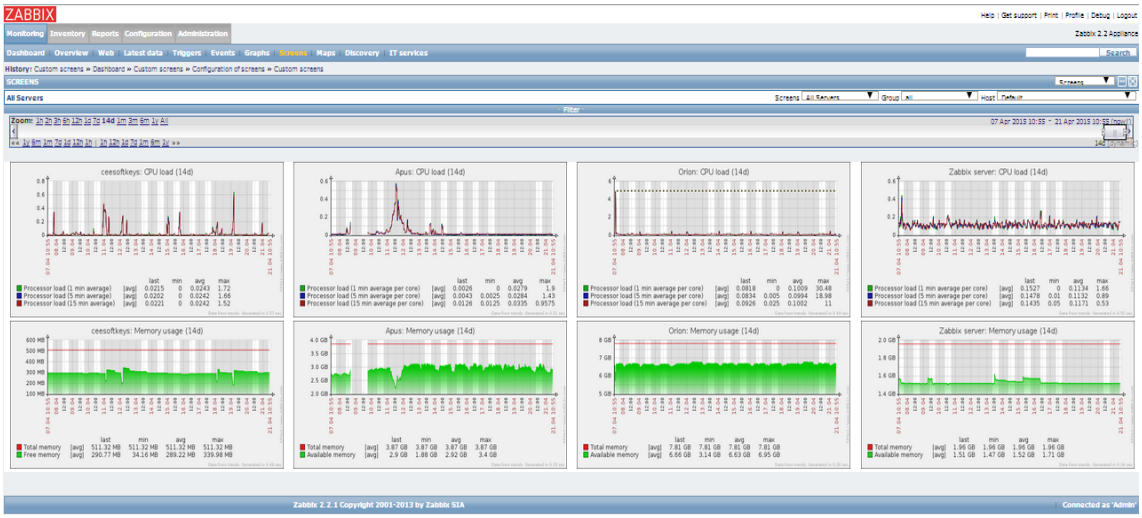


Figura 21 – Vista do estado dos servidores (14d)

2. Possibilitar uma gestão correctiva, agindo rapidamente sobre os problemas detectados e optimizando o tempo da sua resolução.

Embora não existam tempos de referência para se conseguir fazer uma comparação a nível quantitativo, uma vez que não existem registos do tempo que os administradores despendiam a corrigir uma eventual falha, pode-se afirmar que, antes da implementação da solução no CCCEE, o administrador demorava mais tempo a responder a um problema, pois muitas vezes esses problemas só eram do seu conhecimento após a existência de queixas dos utilizadores. Através da solução implementada, o administrador consegue saber mais rápidamente quando, onde, e que tipo de problema foi detectado na rede, pela ferramenta de monitorização, podendo desta forma fornecer uma resposta mais rápida e eficiente aos problemas identificados.

Por exemplo, quando o servidor de licenças de *software* (*ceesoftkeys*) ficava indisponível, o normal funcionamento de algumas actividades de ensino e de investigação fica comprometido, uma vez que este servidor fornece o serviço de licenças responsável por permitir a operacionalidade dos softwares de apoio a essas mesmas actividades.

Antes da implementação desta solução, a detecção da indisponibilidade do servidor *ceesoftkeys* era notificada, por diversas vezes, pelos próprios membros do corpo docente do CCCEE durante o horário das actividades de ensino.

Com a ferramenta de gestão e monitorização implementada no campus informático do CCCEE, as máquinas são monitorizadas constantemente automaticamente através de um ping realizado pelo próprio Zabbix. Em cada momento que o sinal desapareceu, representado pelas áreas em branco na Figura 22, correspondeu ao despoletar de um alerta e ao envio de um *e-mail* ao administrador do CCCEE – como definido anteriormente no esquema da Figura 14 na secção 4.3.1 –, a notificar este último da indisponibilidade do serviço de licenças de *software,* o que veio permitir uma intervenção mais rápida ao problema.

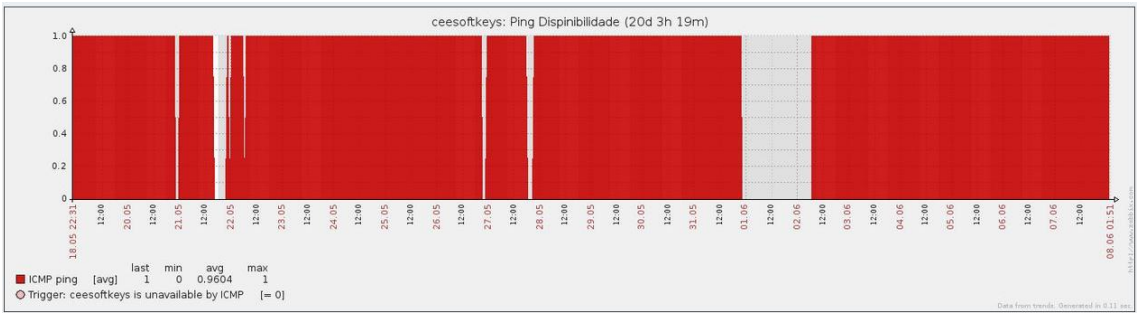


Figura 22 - Gráfico da Disponibilidade do Servidor ceesoftkeys (20d 3h 19m)

Outro exemplo refere-se à monitorização do sistema de ficheiros, na Figura 23, em que quando o valor de espaço livre em disco é menor que 20%, o sistema de gestão e monitorização lança um *trigger* e notifica o administrador do CCCEE dessa mesma ocorrência.

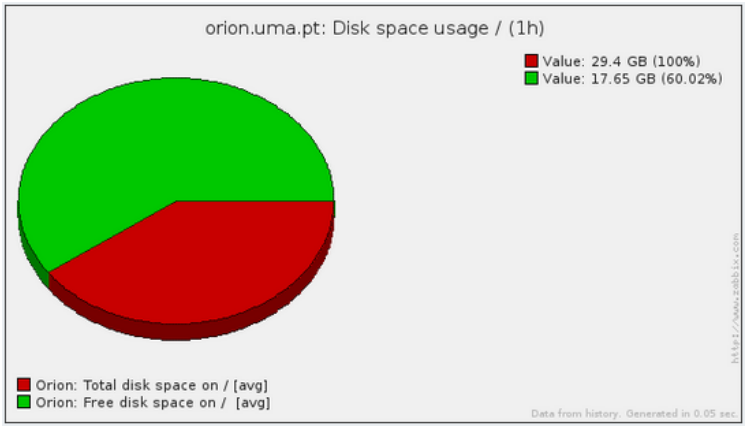


Figura 23 – Estado do Sistema de ficheiros do Servidor Orion (1d)

Outro factor também importante na tarefa de gestão e monitorização de uma rede informática é garantir que o próprio sistema de gestão e monitorização encontra-se a funcionar correctamente, sem quebras no desempenho. Por esta razão, o administrador do CCCEE é notificado de alguns alertas que o ajudam a perceber quando o Zabbix pode estar a perder desempenho.

Por exemplo, quando o número de *queries* à base de dados MySQL do Zabbix, na Figura 24, ultrapassa as 30 qps (*queries per second*) e/ou quando a execução de um processo de recolha de dados do Zabbix ultrapassa os 70%, apresentado na Figura 25, é lançado um *trigger* para cada uma das ocorrências e o administrador do CCCEE é notificado por *e-mail*.

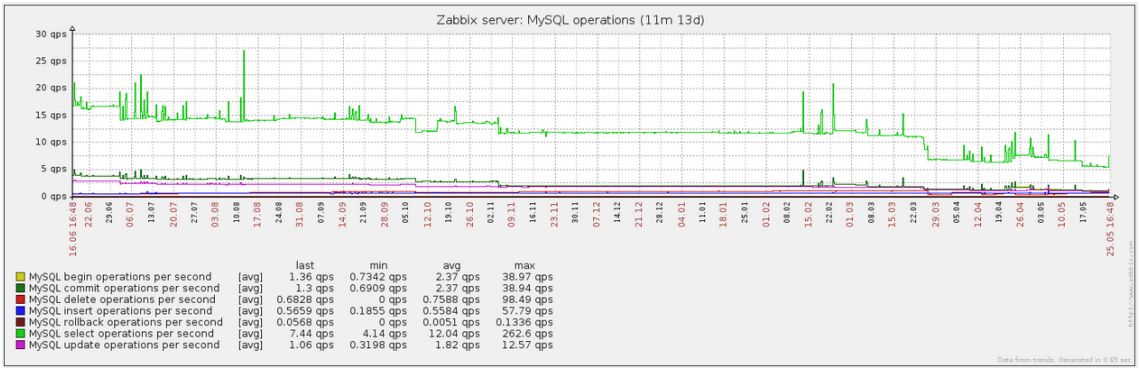


Figura 24 - Gráfico das Operações MySQL no Servidor do Zabbix (11M 13d)

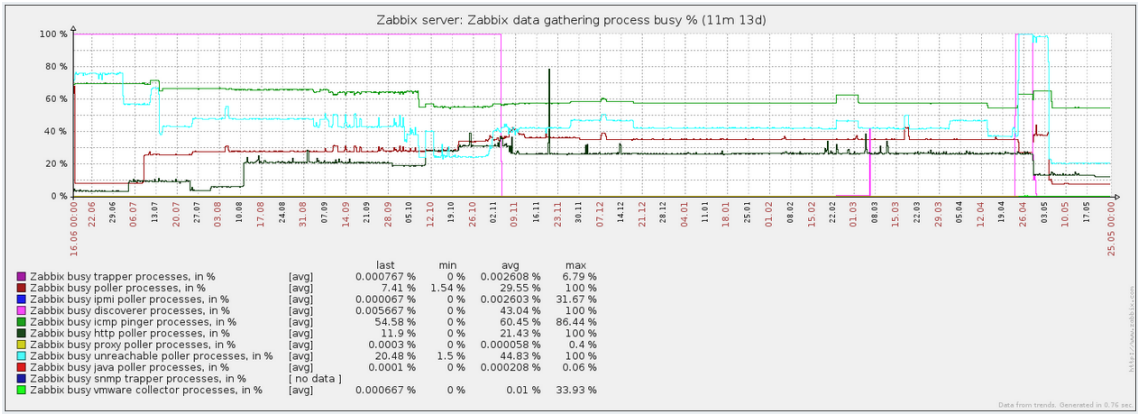


Figura 25 - Processo de recolha de dados do Zabbix (11M 13d)

No entanto, nem todos os eventos detectados pela solução geram alertas, nem os gestores do CCCEE são notificados no exacto instante em que ocorrem. Por exemplo, os eventos gerados por problemas classificados com grau de gravidade “Sem Classificação” e “Informação” (ver Capítulo 4), estes ficam apenas registados na aplicação de gestão e monitorização, e a informação da sua ocorrência poderá ser posteriormente consultada na aplicação por ambos os gestores do CCCEE.

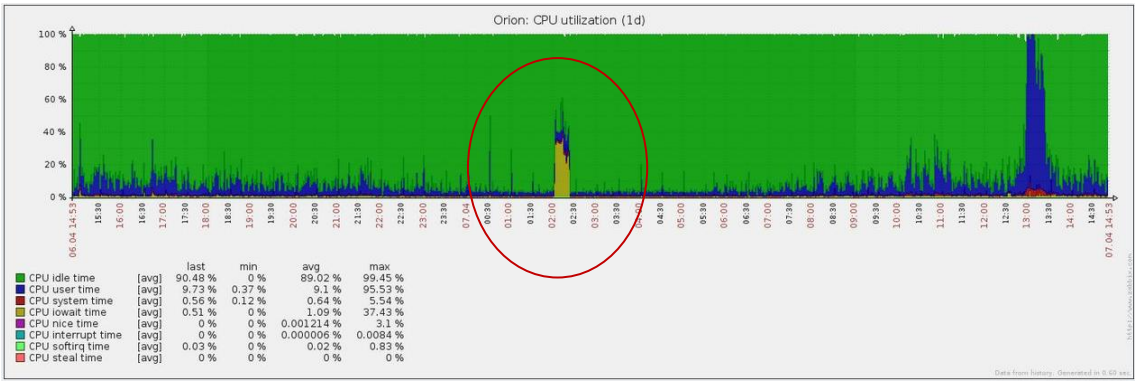


Figura 26 - Gráfico da utilização do CPU no Servidor Orion (1d)

O administrador do CCCEE só é notificado que o Disk I/O está sobrecarregado apenas se, nos últimos 5 minutos o valor médio monitorizado for maior que 30%, o que poderá ser um indicador de problemas de desempenho relacionados com o sistema de armazenamento.

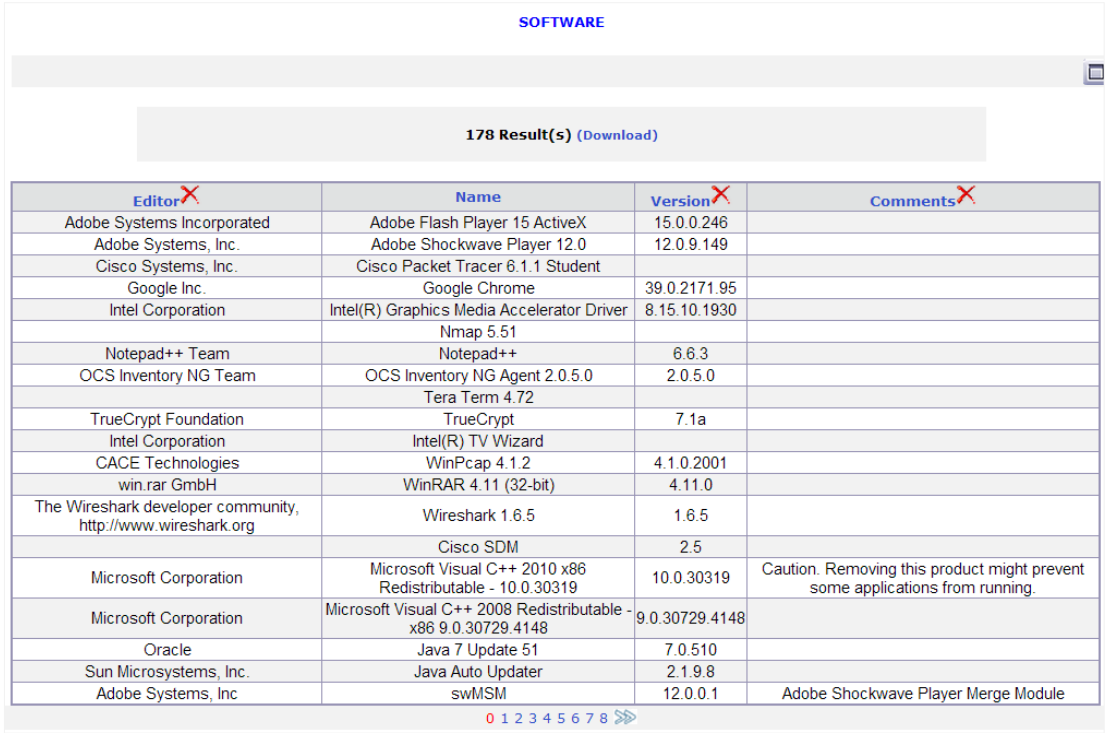
No entanto, para a situação em particular do servidor Orion, a notificação de um alerta sobre o Disk I/O sobrecarregado, representado a amarelo e assinalado com um círculo na Figura 26, indica ao administrador do CCCEE que os *backups* foram realizados.

3. *Melhorar a informação de quais os recursos (hardware e software) que existem nas instalações do CCCEE.*

Com o sistema de gestão de inventário implementado no campus informático do CCCEE, foi possível fornecer aos administradores um conjunto de informações sobre os vários tipos de sistemas integrados na rede e, ainda, tornar a função de criar e manter o inventário actualizado numa tarefa mais rápida, uma vez que o respectivo processo passa maioritariamente a ser executado de forma automatizada pelo sistema de gestão de inventário.

A nível do *hardware*, com a informação adquirida, o administrador consegue saber o número total de equipamentos que existem a funcionar na rede, assim como a descrição dos componentes físicos e lógicos que constituem cada um dos mesmos.

Uma limitação da solução de inventário respectivamente aos recursos de *hardware*, trata-se de não ser possível registar-se periféricos de saída (projectores, colunas e monitores de computadores) e periféricos de entrada (teclados, ratos, microfones e webcams), que não se encontrem conectados a um qualquer sistema com condições para poder ser registado na aplicação, não existindo por essa razão informações dados quantitativos dos respectivos equipamentos.



SOFTWARE

178 Result(s) (Download)

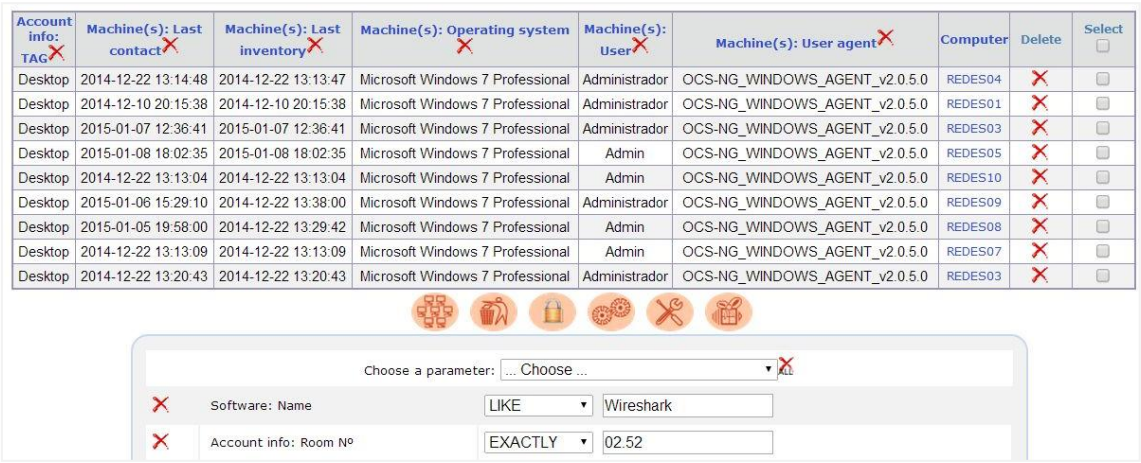
Editor	Name	Version	Comments
Adobe Systems Incorporated	Adobe Flash Player 15 ActiveX	15.0.0.246	
Adobe Systems, Inc.	Adobe Shockwave Player 12.0	12.0.9.149	
Cisco Systems, Inc.	Cisco Packet Tracer 6.1.1 Student		
Google Inc.	Google Chrome	39.0.2171.95	
Intel Corporation	Intel(R) Graphics Media Accelerator Driver	8.15.10.1930	
	Nmap 5.51		
Notepad++ Team	Notepad++	6.6.3	
OCS Inventory NG Team	OCS Inventory NG Agent 2.0.5.0	2.0.5.0	
	Tera Term 4.72		
TrueCrypt Foundation	TrueCrypt	7.1a	
Intel Corporation	Intel(R) TV Wizard		
CACE Technologies	WinPcap 4.1.2	4.1.0.2001	
win.rar GmbH	WinRAR 4.11 (32-bit)	4.11.0	
The Wireshark developer community, http://www.wireshark.org	Wireshark 1.6.5	1.6.5	
	Cisco SDM	2.5	
Microsoft Corporation	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319	10.0.30319	Caution. Removing this product might prevent some applications from running.
Microsoft Corporation	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	9.0.30729.4148	
Oracle	Java 7 Update 51	7.0.510	
Sun Microsystems, Inc.	Java Auto Updater	2.1.9.8	
Adobe Systems, Inc	swMSM	12.0.0.1	Adobe Shockwave Player Merge Module

0 1 2 3 4 5 6 7 8

Figura 27 - Informação do *software* instalado num computador, recolhidos pelo OCS Inventory

Por sua vez, a documentação do *software*, na Figura 27, possibilitou ainda aos administradores ter o conhecimento sobre o tipo e a versão dos softwares que estão instalados em cada equipamento a operar na rede.

Consequentemente, com esta informação, torna-se mais simples verificar, por exemplo, se os computadores existentes nos espaços para as actividades de ensino e investigação, contêm (ou não) o *software* necessário para o apoio das matérias de determinadas disciplinas que requerem softwares específicos (como observado na Figura 28), uma vez que esta verificação não tem que ser realizada de forma manual e individualmente de computador em computador. Adicionalmente, também é possível saber quantos e quais os tipos de máquinas que se encontram numa determinada área das instalações do CCCEE.



Account info: TAG	Machine(s): Last contact	Machine(s): Last inventory	Machine(s): Operating system	Machine(s): User	Machine(s): User agent	Computer	Delete	Select
Desktop	2014-12-22 13:14:48	2014-12-22 13:13:47	Microsoft Windows 7 Professional	Administrador	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES04		
Desktop	2014-12-10 20:15:38	2014-12-10 20:15:38	Microsoft Windows 7 Professional	Administrador	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES01		
Desktop	2015-01-07 12:36:41	2015-01-07 12:36:41	Microsoft Windows 7 Professional	Administrador	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES03		
Desktop	2015-01-08 18:02:35	2015-01-08 18:02:35	Microsoft Windows 7 Professional	Admin	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES05		
Desktop	2014-12-22 13:13:04	2014-12-22 13:13:04	Microsoft Windows 7 Professional	Admin	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES10		
Desktop	2015-01-06 15:29:10	2014-12-22 13:38:00	Microsoft Windows 7 Professional	Administrador	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES09		
Desktop	2015-01-05 19:58:00	2014-12-22 13:29:42	Microsoft Windows 7 Professional	Admin	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES08		
Desktop	2014-12-22 13:13:09	2014-12-22 13:13:09	Microsoft Windows 7 Professional	Admin	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES07		
Desktop	2014-12-22 13:20:43	2014-12-22 13:20:43	Microsoft Windows 7 Professional	Administrador	OCS-NG_WINDOWS_AGENT_v2.0.5.0	REDES03		

Choose a parameter: ... Choose ...

Software: Name | LIKE | Wireshark

Account info: Room Nº | EXACTLY | 02.52

Figura 28 - Resultados da pesquisa de inventário na aplicação OCS Inventory

Um dos principais testes realizados no decorrer deste trabalho foi o de confirmar a fidedignidade dos dados disponibilizados pela solução de inventário. Para esse fim, comparam-se os dados recolhidos manualmente de 2 computadores, com os mesmos dados disponibilizados desta vez pela própria aplicação, tendo-se confirmado que os resultados adquiridos pelos dois métodos correspondiam.

Efectuou-se, ainda, um outro teste para confirmar se a actualização automática dos inventários era executada dentro do intervalo de tempo definido pelo administrador da rede. Deste modo, atribuiu-se diferentes frequências de actualização a um conjunto de computadores e registou-se, durante um determinado período de tempo, se os dados dos inventários de cada equipamento eram actualizados automaticamente de acordo com a frequência previamente estabelecida. As frequências utilizadas entre cada actualização, durante a realização destes testes, variaram entre o intervalo de tempo de 1 dia (valor mínimo suportado pela aplicação) até 1 semana; tendo-se confirmado, após os testes, a viabilidade da funcionalidade de actualização automática dos inventários.

O facto de os administradores poderem contar com uma documentação correcta e actualizada, relativa aos vários recursos de *hardware* e *software* do CCCEE, permite melhores tomadas de decisões referentes, por exemplo, à troca e aquisição de novos sistemas, à execução de configurações e, ainda, um melhor controlo na aquisição ou actualização das licenças dos *softwares*.

Gestão de Alertas

Genericamente, um típico sistema de alertas permite minimizar o impacto provocado por algum problema. Mas, na prática, se esse sistema não estiver bem configurado verifica-se que muitas vezes, dependendo do tipo ou da regra de avaliação definida, os gestores de rede podem ser notificados mesmo quando tudo está a funcionar correctamente ou de situações que não representam um risco imediato para interferir com o normal funcionamento do sistema informático.

Durante a fase inicial dos testes à solução, utilizou-se os valores fornecidos, por defeito, fornecidos pela aplicação de gestão e monitorização, que definiam quando um evento deveria ser considerado um problema. Após um determinado período de tempo constatou-se que esses valores não se adequavam, em alguns casos, à realidade da infra-estrutura informática do CCCEE. Dos eventos criados pela aplicação, os quatro que geraram mais alertas corresponderam aos seguintes componentes/recursos:

- **Espaço no Disco –** Verifica a percentagem de espaço livre no disco, avaliando se o último valor que a expressão retorna é inferior a 20%.
  - *{Template:vsf.fs.size[{#FSNAME},pfree].last(0)} < 20*

- **Carga CPU –** Verifica a carga do CPU, avaliando, numa média de 5 minutos, se o último valor que a expressão retorna, é superior a 2.
  - *{Template:system.cpu.load[percpu,avg5].last(0)} > 2*

- **Disk I/O sobrecarregado** – Verifica a carga de utilização do CPU, no estado *iowait*, avaliando se o valor médio retornado dos últimos 5 minutos é superior a 30%.
    - *{Template:system.cpu.util[,iowait].avg(5m)} > 30*

- **Agentes Zabbix fora de alcance –** Avalia se não existem dados recebidos pelo agente Zabbix nos últimos 10 minutos.
    - *{Template:agent.ping.nodata(10m)} = 1*

No caso em particular da monitorização do espaço em disco nos servidores, configurou-se o sistema de alertas inicialmente para notificar o administrador quando o espaço no disco fosse inferior a 20%. Contudo, os servidores existentes na rede do CCCEE não têm muito espaço livre em disco e, por esse motivo, esses avisos surgiam muito rapidamente, sendo por essa razão muitas vezes ignorados pelo administrador. Esta situação levava a que os discos ficassem cheios e, consequentemente, a que os servidores deixassem de funcionar normalmente.

Desta forma, alterou-se o valor inicialmente configurado de 20% para os 10%. Esta alteração não "resolveu" inteiramente o problema mas permitiu dar uma folga maior entre cada notificação enviada ao administrador do CCCEE, sobre a falta de espaço no disco. Assim sendo, a expressão adoptada para o *trigger* foi a seguinte:

- **Espaço no Disco**
    - *{Template:vsf.fs.size[{#FSNAME},pfree].last(0)} < 10*

Muitos dos alertas gerados pelos outros três componentes mencionados anteriormente, ocorreram devido ao facto do Zabbix não disponibilizar a funcionalidade de detecção de *flappings*. Ou seja, sempre que os valores monitorizados nos três componentes variavam entre o valor limite definido nos respectivos *triggers*, era enviado um alerta aos gestores do CCCEE a notificar a existência desse problema. Por este motivo, para diminuir o número de notificações enviadas, foi necessário realizar um trabalho contínuo de afinações das regras de avaliação de cada *trigger*, de modo a conseguir adequar a expressão do *trigger* a cada uma das situações.

Esse processo de afinação demorou algum tempo e implicou a utilização de expressões lógicas mais complexas ('*hysteresis*'). Após uma série de afinações às expressões dos *triggers*, chegou-se às seguintes expressões lógicas **(A | B)**:

- **Carga CPU**

A. ({TRIGGER.VALUE}=0 & {Template:system.cpu.load[percpu,avg5].avg(15m)}>2) |
B. ({TRIGGER.VALUE}=1 & {Template:system.cpu.load[percpu,avg5].avg(15m)}>1.5)

- **Disk I/O sobrecarregado**

A. ({TRIGGER.VALUE}=0 & {Template:system.cpu.util[,iowait].avg(5m)}>40) |
B. ({TRIGGER.VALUE}=1 & {Template:system.cpu.util[,iowait].avg(5m)}>30)

- **Agente Zabbix fora de alcance**

A. ({TRIGGER.VALUE}=0 & {Template:agent.ping.nodata(1h)}=1) |
B. ({TRIGGER.VALUE}=1 & {Template:agent.ping.nodata(24h)}=1)

A primeira condição **'A'**, das expressões definidas anteriormente, determina quando um evento deve passar do estado 'ok = 0' para o estado 'problema = 1', enquanto a segunda condição **'B'** define até quando esse evento deve permanecer no estado de problema.

Com a nova afinação das expressões, o *trigger* deixa ainda de avaliar o último dado monitorizado, passando a avaliar o resultado médio dos valores monitorizados no intervalo de tempo definido.

Os gestores do CCCEE são, então, apenas notificados quando o resultado da expressão lógica do *trigger* **(A | B)** for verdadeiro, tendo-se desta forma conseguido diminuir o número de notificações para menos de metade das inicialmente enviadas.

5.2. Conclusão

Neste capítulo, apresentou-se os testes e os resultados obtidos após a implementação das soluções de gestão e monitorização da rede. Embora não se tenha utilizado a capacidade total das soluções de gestão e monitorização implementadas na infra-estrutura informática do CCCEE, os resultados adquiridos dos testes efectuados mostraram-se, no global, suficientes para poder concluir-se que ambas as ferramentas conseguem responder, no geral, aos objectivos definidos no início deste projecto.

A utilização da solução de gestão e monitorização implementada no CCCEE permitiu adquirir informação de diferentes tipos de dados sobre os vários sistemas do campus informático do CCCEE, o que auxiliou os gestores da rede do CCCEE na tomada de decisões acerca, por exemplo, da aquisição de novos equipamentos ou na troca de recursos entre máquinas.

Embora não existam tempos de referência, o facto dos gestores do CCCEE serem notificados sobre os diferentes tipos de problemas, por exemplo: falta de espaço no disco, excesso de carga e utilização do CPU, assim como da indisponibilidade dos sistemas; possibilitou aos gestores do CCCEE actuar de forma mais rápida sobre os problemas identificados e, desta forma, diminuir o impacto desses mesmos problemas na qualidade dos serviços disponibilizados aos utilizadores do CCCEE, garantindo assim uma gestão mais pró-activa e correctiva de toda a rede informática.

6. Conclusões

6.1. Conclusões

Perceber a composição e a estrutura de uma infra-estrutura informática, assim como ter a capacidade de, a cada momento, estar informado sobre a disponibilidade e o desempenho de cada elemento que a compõe, pode ser o factor decisivo para o sucesso da integridade e disponibilidade de uma rede informática.

A abordagem às arquitecturas de gestão de redes OSI e TMN, e principalmente à arquitectura de gestão da internet TCP/IP, permitiram perceber como os sistemas integrados numa rede informática comunicam e partilham informações entre si. Identificou-se, ainda, que os modelos presentes em cada uma das arquitecturas mencionadas anteriormente servem de base para várias ferramentas de gestão e monitorização de redes, que seguem o modelo gestor-agente e utilizam o protocolo SNMP, de forma a abranger o maior número de sistemas numa rede para gerir e monitorizar. De um modo geral, pode-se afirmar que as ferramentas de gestão e monitorização de redes são as principais responsáveis pelo grau de controlo dos equipamentos, aplicações e serviços possíveis de abranger.

Um factor de grande relevância de todo o desenvolvimento do presente projecto, foi a necessidade de realizar-se primeiro o estudo das características da rede do CCCEE. Esta tarefa não foi simples, tendo demorado algum tempo e envolvido particularmente várias reuniões com o então gestor da rede do CCCEE. No entanto, permitiu entender a estrutura e o funcionamento da rede e fazer o levantamento dos problemas existentes e das necessidades na área da monitorização e gestão da rede e dos serviços.

A escolha das ferramentas foi também uma fase complexa de todo o processo que envolveu a gestão e monitorização da infra-estrutura do CCCEE, uma vez que abrangeu a análise e comparação de várias funcionalidades de um largo conjunto de ferramentas disponibilizadas actualmente no mercado, para que fosse possível selecionar a que mais se adequava à realidade do CCCEE, tentando dessa forma assegurar a melhor relação custo-benefício.

O processo de aprendizagem/adaptação às ferramentas foi apoiado, inicialmente, pela documentação disponibilizada *online,* tendo sido necessário despender-se algum tempo para que fosse possível entender e perceber o funcionamento das diversas funcionalidades disponibilizadas e o significado dos vários conceitos existentes em cada uma das ferramentas, mas principalmente perceber como esses mesmos conceitos se relacionavam e interagiam entre si.

Mas, foi na fase de testes às ferramentas que se conseguiu conhecer, com maior detalhe, o funcionamento das várias funcionalidades disponibilizadas pelas soluções implementadas. Foi também na fase de testes que surgiram algumas dificuldades; nomeadamente no processo de afinação das regras de avaliação dos dados monitorizados, pois é importante garantir que o

sistema de gestão de alertas se encontra bem configurado, uma vez que, uma simples regra que cause falsos positivos pode facilmente gerar centenas de alertas num pequeno espaço de tempo, sendo que o administrador poderá receber notificações frequentes mesmo que a infra-estrutura informática esteja a funcionar perfeitamente.

De um modo sucinto, antes da implementação desta solução, pode-se afirmar que não existiam nas instalações do CCCEE, qualquer método de monitorização e gestão das tecnologias de informação do mesmo, sendo que as tarefas de verificação e análise do comportamento e estado da rede eram realizadas pontualmente e em grandes intervalos de tempo. Constatou-se que, em várias situações, os administradores da rede apenas agiam quando já existiam problemas no funcionamento da rede e na indisponibilidade dos serviços aos utilizadores. Com o desenvolvimento do presente projecto, os administradores da rede são dotados de mecanismos para conseguirem se aperceber mais cedo de alguma situação fora do comportamento normal (por ex., indisponibilidade dos serviços, carga do CPU de um servidor), e agir antes que os problemas ocorram ou prejudiquem o correcto funcionamento das actividades de ensino e investigação do CCCEE.

O facto de esta solução possibilitar a detecção e a identificação mais rápida dos problemas e, consequentemente, uma intervenção/resolução dos problemas mais cedo, veio permitir aos administradores monitorizar e acompanhar diariamente, de forma mais fácil e rápida, o comportamento e desempenho das TI existentes no CCCEE, garantindo assim uma gestão mais preventiva e correctiva de toda a infra-estrutura informática.

Embora a solução de gestão de inventário, implementada na rede do CCCEE, não tenha conseguido responder a todos os requisitos, como por exemplo, não permitir adicionar um novo registo de um componente individual (i.e. teclados, ratos, ecrãs, *motherboards*, memórias, CPU, entre outros), possibilitou no entanto: 1) melhorar o controlo do *stock* existente, 2) fornecer informação detalhada sobre cada recurso (*hardware* e *software*), 3) identificar situações de renovação e pagamento de licenças de *software* e, 4) ajudar na tomada de decições sobre a necessidade da aquisição de novos recursos.

Com base na informação adquirida no desenvolvimento deste projecto, consegue-se concluir que a criação de uma estratégia de gestão preventiva e correctiva de todos os serviços e tecnologias de informação é, muitas vezes, a "chave mestra" para se possuir uma rede robusta e fiável, possibilitando uma redução de custos bem como o crescimento dos serviços já existentes na rede.

6.2. Trabalhos Futuros

De um modo geral, as tomadas de decisão realizadas durante o desenvolvimento do presente projecto focaram-se, maioritariamente, em dar resposta aos problemas que necessitavam de uma intervenção mais rápida, nomeadamente nas áreas de gestão de falhas, gestão de configuração e gestão de desempenho. Assim sendo, o trabalho a desenvolver numa próxima fase, deverá passar também por cobrir as outras áreas funcionais do modelo FCAPS, i.e. a área de gestão de contabilização e a área de gestão da segurança.

Por não ter existido condições para ser possível abranger todos os equipamentos e serviços do CCCEE pela ferramenta de gestão e monitorização, o trabalho deve continuar por uma das seguintes alternativas:

- Configurar o *proxy* do Zabbix na rede dos docentes, como exemplificado na Figura 12 na secção 4.3 da Arquitectura da Solução, para que os sistemas a operar na rede dos docentes sejam monitorizados e geridos pela ferramentas Zabbix, ou;

- Como alternativa, como as dimensões da rede do CCCEE não justificam a implementação de uma monitorização distribuída, através da utilização de um *proxy*, a solução ideal passaria atribuir à máquina que aloja o servidor do Zabbix na rede dos alunos, permissão para poder actuar nos sistemas integrados na rede dos docentes. Desta forma todos os sistemas a operar na infra-estrutura informática do CCCEE passariam a estar abrangidos pelos dois sistemas de gestão implementados;

Adicionalmente propõe-se também a execução, por parte dos administradores do CCCEE, de todas as boas práticas dos cinco estados do ciclo de vida de um serviço do Modelo ITIL – descrito na secção 2.3 –, nomeadamente: Estratégia de Serviço (*Service Strategy*), *Design* de Serviço (*Service Design),* Serviço de Transição (*Service Transition),* Serviço de Operação *(Service operation)* e, finalmente, o estado Melhoria Continua do Processo (*Continual Process Improvement*). Para além disso, também se propõe, a implementação da norma internacional ISO/IEC 20000, de forma a que a organização possa ser certificada em termos da qualidade dos serviços de TI fornecidos.

Referências

[1] I. 7498-1, “Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model,” 1994.

[2] ITU-T. M.3010, “Principles for a telecommunications management network,” 2000.

[3] “ISO. ISO/IEC 7498-4 Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management framework,” 1989.

[4] “ISO. ISO/IEC 10040 Information technology - Information technology - Open Systems Interconnection,” 1998.

[5] “ISO. ISO/IEC 7498-1 Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model,” 1996.

[6] E. M. D. Marques, “Interoperabilidade e optimização da Gestão de Redes com a Framework NSDL,” Funchal, 2013.

[7] ITU-T. M3200 , “TMN management services and telecomunications managed areas: overview,” 2000.

[8] “RFC Editor,” [Online]. Available: http://www.rfc-editor.org/. [Acedido em 2 Outubro 2014].

[9] “RFCs de TCP/IP,” [Online]. Available: http://technet.microsoft.com/pt-BR/library/cc737968(v=ws.10).aspx. [Acedido em 2 Outubro 2014].

[10] F. Boavida, M. Bernandes e P. Vapi, Administração de Redes Informáticas, 2ª ed., Lisboa: FCA - Editora de Informática, Março 2011.

[11] E. Monteiro e F. Boavida, Engenharia de Redes Informáticas, 10ª ed., Lousã: FCA - Editora de Informática, Fevereiro 2011.

[12] P. Goyal, R. Mikkilineni e M. Ganti, “FCAPS in the Business Services Fabric Model,” 2009.

[13] H.-G. Hegerind, S. Abeck e B. Neumair, Integrated Management of Networked Systems, San Francisco, California: Morgan Kaufmann Publishers, 1999.

[14] M. Subramanian, Network Management Principles and Practice, K. Harutunian, Ed., Califórnia: Addison-Wesley, 2000.

[15] F. Boavida e M. Bernandes, “Gestão de Redes (SNMP),” em *TCP/IP Teoria e Prática*, Lisboa, FCA - Editora de Informática, Lda, Junho 2012, pp. 358-366.

[16] J., Case; M., Fedor; M., Schoffstall; J., Davin, “rfc-1157 IETF,” Maio 1990. [Online]. Available: https://www.ietf.org/rfc/rfc1157.txt. [Acedido em 15 Outubro 2014].

[17] J. R. Burke, Network Management Concept and Pratice: A Hands-on Approach, New Jersey: Person Education, Inc., 2004.

[18] T. C. Piliouras, Network Design, Management and Technical Perspectives, 2ª ed., USA: Auerbach, 2004.

[19] A. Cartlidge, C. Rudd, M. Smith, P. Wigzel, S. Rance, S. Shaw e T. Wright, “An Introductory Overview of ITIL® 2011,” London, 2012.

[20] J. v. Bon, A. d. Jong, A. Kolthof, M. Pieper, R. Tjassing, A. v. d. Veen e T. Verheijen, ITIL Version 3 - A Pocket Guide, Van Haren Publishing, 2009.

[21] A. Cartlidge, A. Hanna, C. Rudd, I. Macfarlane, J. Windebank e S. Rance, “An Introductory Overview of ITIL® V3,” 2007.

[22] M. Szaniawski, “ITIL Continual Service Improvement,” [Online]. Available: http://www.css-security.com/blog/itil-continual-service-improvement/. [Acedido em 15 Maio 2015].

[23] S. Taylor, M. Iqbal e M. Nieves, “ITIL Version 3 Service Strategy,” 2007.

[24] S. Taylor, V. Lloyd e C. Rudd, “ITIL Version 3 Service Design,” 2007.

[25] S. Taylor, S. Lacy e I. Macfarlane, “ITIL Version 3 Service Transition,” 2007.

[26] S. Taylor, D. Cannon e D. Wheeldon, “ITIL Version 3 Service Operation,” 2007.

[27] S. Taylor, G. Case e G. Spalding, “ITIL Version 3 Continual Service Improvement,” 2007.

[28] M. Rovers, ISO/IEC 20000:2011 - A Pocket Guide, 2ª ed., J. Chittenden, Ed., Van Haren Publishing, 2013.

[29] G. Harmer, Governance of Enterprise IT Based on COBIT 5: A Management Guide, IT Governance, 2014.

[30] Kempter, Stefan; Kempter, Andrea;, “Introduction ISO 20000 and the ITIL® - ISO 20000 Bridge,” 2013. [Online]. Available: http://en.it-processmaps.com/media/introduction_itil_iso_20000_bridge.pdf. [Acedido em 13 Outubro 2014].

[31] S. D. V. Hove e M. Thomas, Pragmatic Application of Service Management: The Five Anchor Approach, It Governance Limited, 2014.

[32] “Comparison of network monitoring systems,” 10 Setembro 2014. [Online]. Available: http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems. [Acedido em 19 Novembro 2014].

[33] “FindTheBest,” 2014. [Online]. Available: http://network-management.findthebest.com/ . [Acedido em 22 Novembro 2014].

[34] OTRS AG, “OTRS::ITSM 4,” 2014.

[35] GLPI, “GLPI Free IT and Asset Management Software,” [Online]. Available: http://www.glpi-project.org/spip.php?article43. [Acedido em 12 Março 2014].

[36] T. Urban, Cacti 0.8 Beginner's guide, Packt Publishing Ldt., 2011.

[37] D. Kundu e S. M. I. Lavlu, Cacti 0.8 Network Monitoring, Packt Publishing Ltd., 2019.

[38] SecurActive Performance Vision, “Graphing Network & Application Performance with Cacti and Nagios,” 5 Dezembro 2012. [Online]. Available: http://blog.securactive.net/graphing-network-application-performance-cacti/cacti_performance_vision/. [Acedido em 16 Maio 2014].

[39] C. B. Rockwood, “Getting Started with RRDtool,” 10 Maio 2004. [Online]. Available: http://www.cuddletech.com/articles/rrd/rrdintro.pdf. [Acedido em 19 Maio 2014].

[40] “Cacti documentation and howtos,” 10 Janeiro 2011. [Online]. Available: http://docs.cacti.net/manual:087:2_basics.0_principles_of_operation. [Acedido em 21 Maio 2014].

[41] “Cacti documentation and howtos,” 28 Setembro 2010. [Online]. Available: http://docs.cacti.net/plugins. [Acedido em 29 Novembro 2014].

[42] V. Mehta, Icinga Network Monitoring, Packt Publishing Ltd., 2013.

[43] W. Kocjan, Learning Nagios 4, Packt Publishing Ltd., 2014.

[44] T. Mobily, “Nagios and Icinga,” *Nagios Vs. Icinga: the real story of one of the most heated forks in free software,* p. 1, 27 Abril 2012.

[45] “Icinga Arquitecture,” [Online]. Available: https://www.icinga.org/about/architecture/ . [Acedido em 2 Maio 2014].

[46] “About NSClient++,” [Online]. Available: http://docs.nsclient.org/manual/about.html. [Acedido em 6 Fevereiro 2014].

[47] “Nagios NRPE Documentation,” 1 Maio 2007. [Online]. Available: http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf. [Acedido em 6 Fevereiro 2014].

[48] A. D. Vacche e S. K. Lee, Mastering Zabbix, Packt Publishing Ltd., 2013.

[49] R. Olups, Zabbix 1.8 Network Monitoring, Packt Publishing Ltd., 2010.

[50] B. T. Antal, IT Inventory and Resource Management with OCS Inventory NG 1.02, Packt Publishing Ltd, 2010.

[51] "Documentation:WindowsAgent," 16 Maio 2013. [Online]. Available: http://wiki.ocsinventory-ng.org/index.php/Documentation:WindowsAgent. [Acedido em 22 Novembro 2013].

[52] "Documentation:Server," 8 Novembro 2012. [Online]. Available: http://wiki.ocsinventory-ng.org/index.php/Documentation:Server. [Acedido em 4 Novembro 2013].

[53] "Documentation:IPDiscovery," 1 Agosto 2012. [Online]. Available: http://wiki.ocsinventory-ng.org/index.php/Documentation:Ipdiscover. [Acedido em 20 Novembro 2013].

[54] "Plugins:version2," 15 Janeiro 2014. [Online]. Available: http://wiki.ocsinventory-ng.org/index.php/Plugins:version2. [Acedido em 3 Março 2014].

[55] "OCS Inventory NG," [Online]. Available: http://www.ocsinventory-ng.org/en/about/features/ocsng-glpi.html. [Acedido em 5 Março 2014].

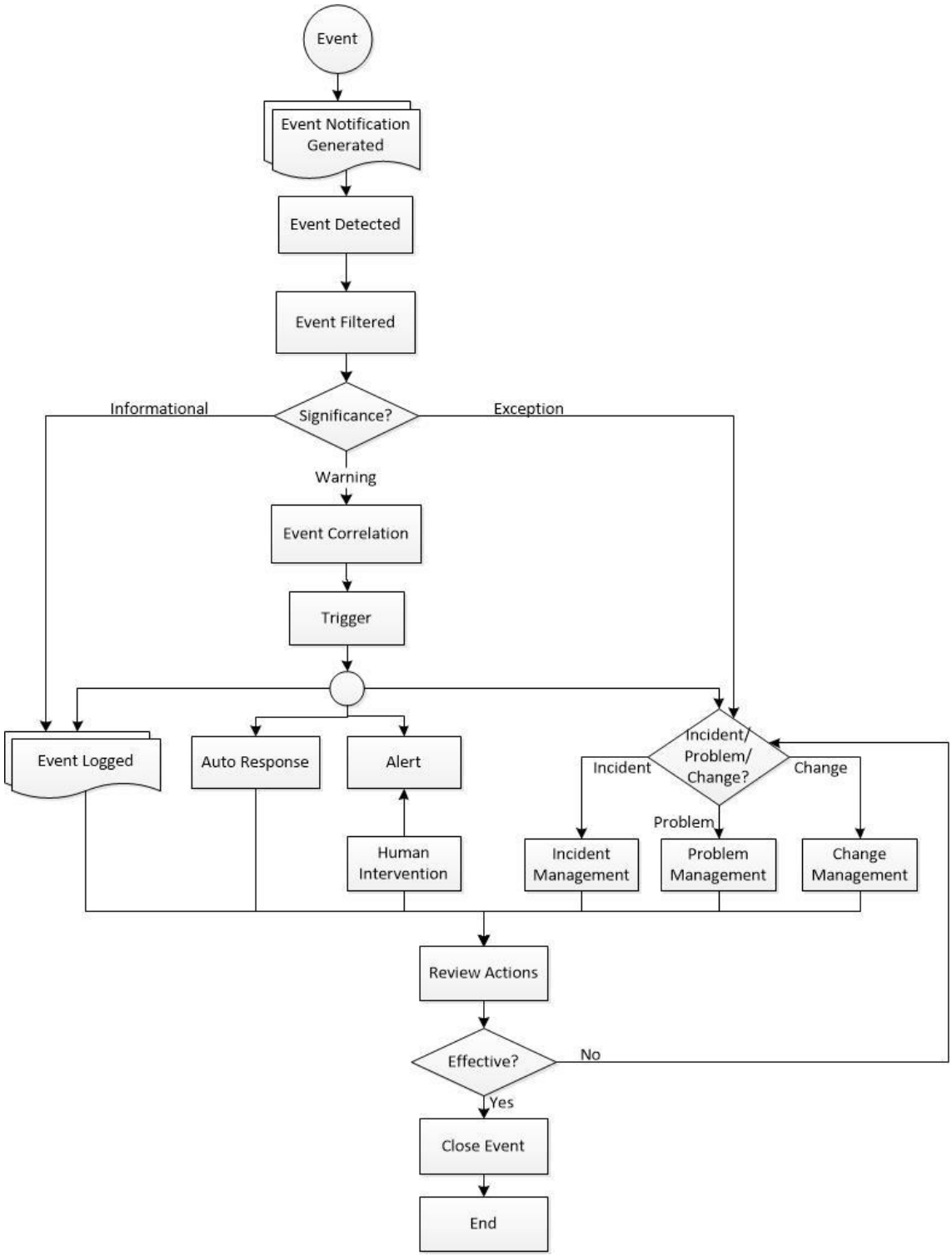
[56] "Enabling the SNMP Agent for Linux SUSE," 11 Fevereiro 2011. [Online]. Available: http://www.ipnetworksetup.com/2011/11/enabling-snmp-agent-for-linux-suse.html. [Acedido em 30 Abril 2015].

[57] J. Lindfors e M. Fleury, JMX: Managing J2EE with Java Management Extensions, USA: Sams Publishing, 2002.

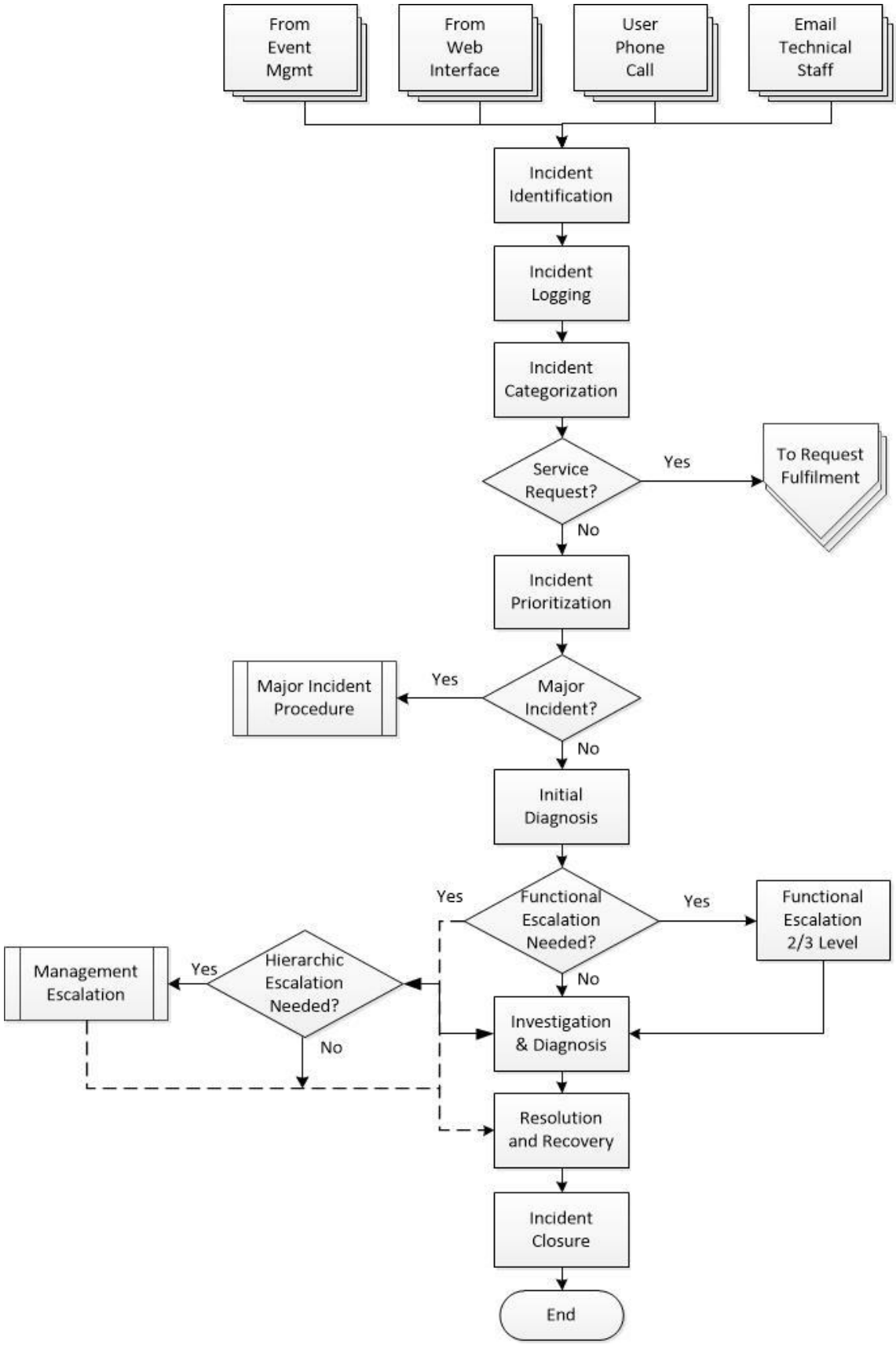
[58] P. Saint-Andre, K. Smith e R. Tronçon, XMPP: The Definitive Guide, USA: O'Reilly Media, Inc., 2009.

Anexos

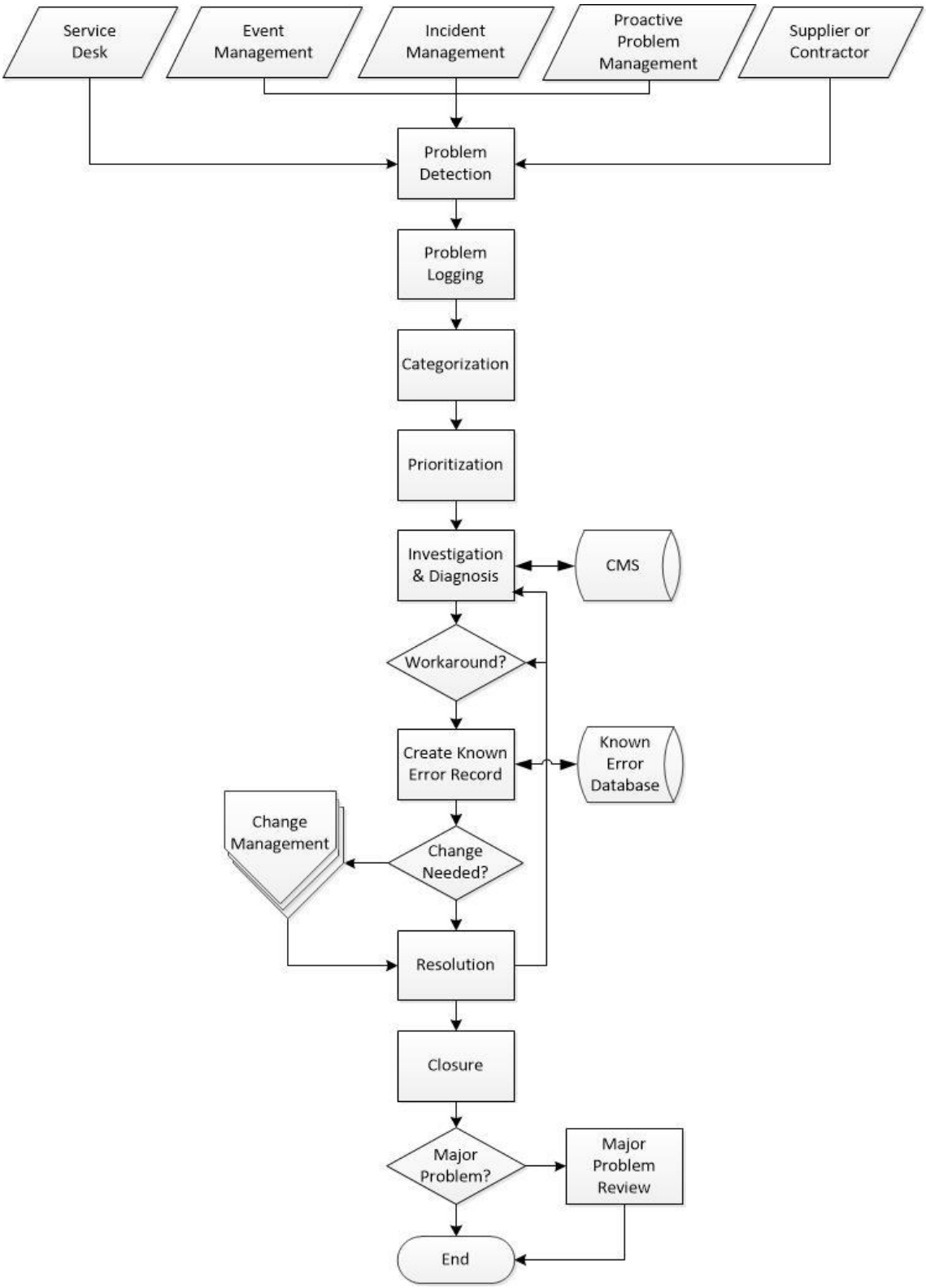
Anexo A. Fluxo de Processos da Gestão de Eventos, pelo ITILv3 [26]



Anexo B. Fluxo de Processos da Gestão de Incidentes, pelo ITILv3 [26]



Anexo C. Fluxo de Processos da Gestão de Problemas, pelo ITILv3 [26]



Anexo D. Habilitação do SNMP, sob o SO Windows

Para habilitar o serviço SNMP num ambiente com o SO Windows, siga os seguintes passos:

1. No **Painel de Controlo**, entre em <**Programas**>, escolha a opção <**Activar ou desactivar funcionalidades do Windows**> e selecione a respectiva caixa de verificação correspondente à funcionalidade SNMP.

2. No próximo passo, ainda no **Painel de Controlo**, entre em <**Sistema e Manutenção**> seguido de <**Ferramentas Administrativas**> e abra a opção <**Serviços**>. Na janela <**Serviços**> entre nas propriedades do '**Serviço SNMP**' e preencha a respectiva informação nas seguintes abas:

   - **Segurança** – adicione as comunidades SNMP aceites e, na opção "*Aceitar pacotes SNMP destes anfitriões"* preencha com o IP do servidor onde se encontra configurado o Zabbix.

   - **Agente** – Selecione todas as caixas de verificação da opção "*Serviço*".

Após realizar as configurações mencionadas, opte por reiniciar o serviço SNMP de modo a garantir que o mesmo funcione com as configurações realizadas.

Anexo E. Habilitação do SNMP, sob o SO Linux

A configuração aqui apresentada, para habilitar o SNMP em ambiente com SO Linux, encontra-se disponibilizada na referência [56].

Para instalar o pacote SNMP, use a fonte de instalação ou o método que considere adequado: **rpm**, **tar** ou usando **yast**.

1. Edite o arquivo snmpd.conf localizado no diretório **/ etc / snmp /** diretório (ou pode ser encontrado no diretório **/ etc /**) com a seguinte informação:

```
rocommunity public 127.0.0.1
#com2sec
com2sec local localhost private
com2sec mynetwork 10.2.15.0/24 public
#group
group local_group v1 local
group local_group v2c local
group local_group usm local
group public_group v1 mynetwork
group public_group v2c mynetwork
group public_group usm mynetwork
view all included .1 80
access local_group "" any noauth exact all none none
access public_group "" any noauth exact all none none
```

2. Salve o arquivo e posteriormente active o SNMP com o comando:

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

Após concluir a configuração o SNMP encontrar-se-á a funcionar e irá iniciar automaticamente quando ligar o computador.

Anexo F. Configuração do agente Zabbix, sob o SO Windows

Para configurar o agente do Zabbix numa máquina com o Sistema Operativo Windows, realize os seguintes passos:

1. Comece por fazer o *download* do arquivo do agente na página do Zabbix.

2. Crie uma pasta com o nome **'zabbix'** no directório **C:\zabbix** e extraia o arquivo transferido.

3. No caminho **C:\zabbix\conf** abra o ficheiro denominado "*zabbix_agentd.win.conf*" e altere os seguintes dados com a respectiva informação:

```
Server= [IP do Servidor Zabbix]
Hostname= [Nome da máquina onde o agente está a ser configurado]
ListenPort = 10050
StartAgents=5
ServerActive = [IP do Servidor Zabbix]
DebugLevel=3
LogFile=C:\Zabbix\zabbix_agentd.log
Timeout=3
```

NOTA: O ficheiro "*zabbix_agentd.win.conf*" contém outros parâmetros por este motivo deve verificar todas as opções disponíveis e alterar mediante a respectiva situação. No entanto os parâmetros apresentados anteriormente deverão ser o conteúdo mínimo preenchido.

4. Em modo Administrador abra a consola de comandos e execute os comandos:

C:\ > cd c:\zabbix\bin\win32 (ou 64, dependendo da arquitectura)
c**:\zabbix\bin\win32 >** zabbix_agentd.exe –i –c c:\zabbix\conf\zabbix_agentd.win.conf

Se tudo estiver correcto, deverá retornar:

```
zabbix_agentd.exe [] : service [Zabbix Agent] installed_successfully
zabbix_agentd.exe [] : event source [Zabbix Agent] installed successfully
```

Procure por fim, na funcionalidade <**Serviços>** do Windows, o serviço **'Zabbix Agent'** e, se este último estiver parado, inicie-o.

Anexo G. Configuração do agente Zabbix, sob o SO Linux

Para configurar o agente do Zabbix numa máquina com o Sistema Operativo Linux (versão Suse), siga os seguintes passos:

1. Com o comando *yast* instale o zabbix_agent através do URL http://software.opensuse.org/download/package?project=server:monitoring&package=zabbix-agent

2. Edite o arquivo **/etc/zabbix_agentd.conf** com os seguintes dados:

```
Server= [IP do Servidor Zabbix]
Hostname= [Nome da máquina onde o agente está a ser configurado]
ListenPort = 10050
StartAgents=5
ServerActive = [IP do Servidor Zabbix]
DebugLevel=3
PidFile=/var/run/zabbix_zabbix_agentd.pid
LogFile=/var/log/zabbix/zabbix_agentd.log
Timeout=3
```

NOTA: O arquivo /etc/zabbix_agentd.conf contém outros parâmetros por este motivo deve verificar todas as opções disponíveis e alterar mediante a respectiva situação. No entanto os parâmetros apresentados anteriormente deverão ser o conteúdo mínimo preenchido.

Por fim, arranque o serviço utilizando o comando:

```
#systemctl enable zabbix-agentd
```