



Sistema de monitorização e alarmística de ativos de rede

CARLOS MIGUEL PORTO DE ALMEIDA

Outubro de 2015

Sistema de monitorização e alarmística de ativos de rede

Carlos Miguel Porto de Almeida

**Dissertação para obtenção do Grau de Mestre em
Engenharia Informática, Área de Especialização em
Arquiteturas, Sistemas e Redes**

Orientador: António Cardoso Costa

Coorientador: Renato Magalhães

Coorientador: Pedro Alvarenga

Júri:

Presidente:

[Nome do Presidente, Categoria, Escola]

Vogais:

[Nome do Vogal1, Categoria, Escola]

[Nome do Vogal2, Categoria, Escola] (até 4 vogais)

Porto, Outubro 2015

Resumo

Este documento contém todo o estudo e planeamento para a implementação de um novo sistema de monitorização e alarmística, desenvolvido para o serviço de informática, no decorrer do estágio profissional no Instituto Português de Oncologia do Porto. Observou-se que o sistema já existente, apesar de facilitar algumas ações da equipa, apresentava muitas lacunas, mas ao mesmo tempo uma boa abertura para evolução.

A criação desse sistema teve que contemplar um conjunto de objetivos que levaram a elaboração de estudos, permitindo uma análise e fundamento na tomada de decisões e na criação de tarefas e testes.

É apresentado também um estudo de uma nova arquitetura, pois devido a falta de recursos que a solução já implementada tinha, que permitisse ao serviço de informática obter um sistema robusto, redundante, fiável, seguro e sempre disponível.

Palavras-chave: Switch, Access Point, UPS, Monitorização, Alarmística

Abstract

This document contains all the study and planning for the implementation of a new monitoring system and alarms, developed for the IT department in the course of internship in the Portuguese Institute of Oncology of Porto. It was observed that the existing system, while facilitating some team's actions, had many shortcomings, but at the same time a good opening for evolution.

The creation of this system has to include a number of goals, that led the elaboration of studies, allowing an analysis and foundation in the decision-making and in the creation of tasks and tests.

It also presents a study of a new architecture, due to the lack of resources allocate to the system that already had implemented, enabling the IT department to obtain a new system that its robust, redundant, reliable, secure and always available.

Keywords: Switch, Access Point, UPS, Monitoring, Alarms

Agradecimentos

Devido ao tempo investido na elaboração deste documento de tese, agradeço a toda a minha família e amigos pelo apoio e consideração pela minha ausência. Quero também agradecer ao meu coordenador de projeto, Professor António Costa, pela sua disponibilidade, ajuda e encaminhamento na redação do presente documento, assim como a todos os elementos da equipa do serviço de informática do IPO Porto pelo tempo disponibilizado na ajuda e apoio na elaboração deste projeto.

Índice

1	Introdução	16
1.1	Enquadramento	16
1.2	Apresentação do projeto/estágio	16
1.3	Apresentação da organização	16
1.4	Contributos deste trabalho	19
1.5	Estruturação do relatório	19
2	Contexto	21
2.1	Problema	21
2.2	Áreas de negócio	22
2.3	Estado da arte	23
2.3.1	Nagios	23
2.3.2	Cacti	26
2.3.3	SpiceWorks	29
2.3.4	Observium	32
2.3.5	Zabbix	35
2.4	Visão da solução	40
3	Ambiente de trabalho	43
3.1	Metodologia de trabalho	43
3.2	Planeamento de trabalho	45
3.3	Tecnologias usadas	46
4	Descrição técnica	47
4.1	Análise e experiências	47
4.1.1	Switch	47
4.1.2	Access Point	48
4.1.3	Uninterruptible power supply	49
4.2	Desenvolvimento da solução e testes	50
4.3	Proposta de solução alternativa	64
5	Conclusões	71
5.1	Resumo do relatório	71
5.2	Objetivos realizados	71
5.3	Outros trabalhos realizados	71
5.4	Limitações e trabalho futuro	72
5.5	Apreciação final	73

5.5.1	Planeamento do trabalho	73
5.5.2	Solução	74
6	Referências	75

Lista de Figuras

Figura 1 - Triângulo estratégico do IPO-Porto	18
Figura 2 - Exemplo de funcionamento de um <i>plugin</i> [Pplware, 2015a]	24
Figura 3 - Interface web do <i>Nagios</i>	25
Figura 4 - Princípio de funcionamento base do Cacti	27
Figura 5 - Interface gráfica do Cacti [Cacti, 2015]	28
Figura 6 - Módulo de Inventário [SpiceWorks, 2015]	30
Figura 7 - Interface gráfica do <i>Spiceworks</i> [SpiceWorks, 2015]	31
Figura 8 - Interface gráfica do Observium[Observium, 2015]	33
Figura 9 - Dados recolhidos pelo Observium [Observium, 2015]	34
Figura 10 - Interface Web do Zabbix.....	36
Figura 11 - Princípio de funcionamento base do Zabbix [Pplware, 2015b]	37
Figura 12 - Posicionamento das aplicações	40
Figura 13 - Metodologia de trabalho do serviço de informática	44
Figura 14 - Gráfico de tráfego	58
Figura 15 - Logica do zabbix	60
Figura 16 - Dashboard do sistema.....	62
Figura 17 - Diagrama da arquitetura em produção	64
Figura 18 - Valores dos novos elementos	65
Figura 19 – Valores dos elementos existentes.....	65
Figura 20 – Diagrama da nova arquitetura	66
Figura 21 – Proposta de configuração do sistema	68
Figura 22 – Listagem hierárquica do identificador de doenças	72

Lista de Tabelas

Tabela 1 - Comparativo de Soluções.....	39
Tabela 2 - Mapa de Grant da fase de desenvolvimento	45
Tabela 3 - Mapa de Grant da fase de transição para produção.....	46
Tabela 4 - Excerto de dados recolhidos da MIB do Switch	48
Tabela 5 - Excerto de dados recolhidos da Mib do Access Point	49
Tabela 6 – Excerto de dados recolhidos da Mib da UPS	50
Tabela 7 - Excerto do estudo do Switch	52
Tabela 8 - Excerto do estudo de alarmística a definir no switch	53
Tabela 9 - Excerto do estudo da UPS	54
Tabela 10 - Excerto do estudo de alarmística a definir nas UPS.....	55
Tabela 11 - Excerto do estudo do Access Point	56
Tabela 12 - Excerto do estudo de alarmística a definir no Access Point.....	57
Tabela 13 – Listagem de gráficos criados.....	59

Acrónimos e Símbolos

Lista de Acrónimos

AP	<i>Access Point</i>
DOS	<i>Disk Operating System</i>
GPL	<i>General Public License</i>
HTML	<i>HyperText Markup Language</i>
IP	<i>Internet Protocol</i>
IPMI	<i>Intelligent Platform Management Interface</i>
JMX	<i>Java Management Extensions</i>
LUN	<i>Logical Unit Number</i>
MIB	<i>Management Information Base</i>
OTRS	<i>Open-source Ticket Request System</i>
PHP	<i>PHP Hypertext Preprocessor</i>
RRDTool	<i>Round-Robin Database Tool</i>
SAN	<i>Storage Area Network</i>
SLA	<i>Service Level Agreement</i>
SNMP	<i>Simple Network Management Protocol</i>
SQL	<i>Structured Query Language</i>
SSH	<i>Secure Shell</i>
TI	Tecnologias de Informação
UPS	<i>Uninterruptible Power Supply</i>

1 Introdução

1.1 Enquadramento

Tendo em conta que a organização pertence a área da saúde e lida com pacientes, enfermeiros e médicos, é necessária a existência de sistemas de informação sofisticados para a gestão dos dados pessoais, médicos, clínicos e outros. Assim sendo, a complexidade da organização e as garantias de segurança que lhe são exigidas implicam a utilização de sistemas de monitorização e alarmística sobre a infraestrutura das redes informáticas.

1.2 Apresentação do projeto/estágio

A necessidade de manter sobre controlo todos os equipamentos existentes na organização é fulcral para que se possa garantir um total funcionamento da mesma. A interligação dos mesmos revela-se também importantíssima. Esta garantia pode ser garantida se toda a rede informática se encontrar em pleno funcionamento. A sua monitorização torna-se então numa mais-valia para todo o sistema, pois permite a gestão, em tempo real, dos recursos e meios que por sua vez garante uma rápida intervenção sobre os problemas.

Os objetivos deste projeto passam pela implementação de um novo sistema que permita monitorizar todos os ativos de rede, criando mecanismos de alerta e auto resolução, no aparecimento de problemas. Ao mesmo tempo capacitar o sistema com uma forma de apresentar a informação donde relações possam ser tiradas em relação a estados e comportamentos, isto de forma simplificada e o mais completa possível.

1.3 Apresentação da organização

O Instituto Português de Oncologia do Porto Francisco Gentil, Entidade Pública Empresarial (IPOPFG, E.P.E.), Centro do Porto foi fundado em abril de 1974 e tem-se *“vindo a distinguir ao longo dos anos pelo dinamismo e lugar cimeiro na qualidade com que acolhe e trata os doentes, pela atividade científica de alta credibilidade que desenvolve e pela qualidade do ensino que realiza na área da oncologia.”* [IPO Porto, 2015a]

Tem como missão “A prestação de cuidados de saúde, em tempo útil, centrados no doente, não descurando a prevenção, a investigação, a formação e o ensino no domínio da oncologia com o objetivo de garantir elevados níveis de qualidade, humanismo e eficiência.” E como visão o estabelecimento de uma política que” Com tempos de tratamento mínimos e taxas de cura máximas, a comunidade verá o doente oncológico como um doente crónico, sem estigmas e com qualidade de vida. A tecnologia ao serviço do doente”. [IPO Porto, 2015b]

Rege-se por um conjunto de valores garantindo que todas as suas decisões são tomadas tendo em vista o melhor interesse das pessoas que serve e emprega.” A estrutura de valores do IPO-Porto abrange cinco vetores:

- *Qualidade – como um hospital do Sistema Nacional de Saúde, a prioridade do IPO-Porto é assegurar serviços de alta qualidade e segurança clínica para as pessoas locais. O IPO-Porto aprenderá com as pessoas que fazem uso dos serviços clínicos, com os recursos humanos da Instituição e com as melhores práticas do SNS e para além dele. Será garantida a qualidade pelo desenvolvimento da força de trabalho, fortalecendo-a para que possa prover cuidados de alta qualidade, segurança e efetividade centrados no paciente.*
- *Integridade – o IPO-Porto tratará os utentes com dignidade e respeito, promovendo a equidade, dando valor à diversidade e oferecendo altos padrões de cuidados de saúde. As decisões serão honestas e responsáveis, no melhor interesse da comunidade que serve. O IPO-Porto promoverá uma força de trabalho que aja de forma aberta e integra. Procurará, constantemente, formas de construir os serviços em torno das necessidades dos utentes, ao mesmo tempo que irá ao encontro das necessidades e expectativas dos colaboradores.*
- *Pessoas – as pessoas estão no coração de todos os serviços do SNS: as pessoas a quem o IPO-Porto serve, as pessoas que emprega, as pessoas que se tornam membros e governantes da Instituição, as pessoas que tornam o sistema passível de financiamento e as pessoas que tornam todo o sistema integrado. Os profissionais são os recursos mais valiosos no hospital. O Instituto estará ao lado do colaborador para que este possa estabelecer um contrato individual com cada paciente, utente, colega, membro, governante e parceiro.*
- *Excelência – o IPO-Porto quer que as pessoas, das mais diversas áreas geográficas ou profissionais, sintam confiança nos serviços prestados pela Instituição. O Instituto*

olhará para o futuro, planeando os seus serviços com base nas necessidades da comunidade local e esperando melhorias contínuas nos resultados dos tratamentos e cuidados que promove. Usará a melhor evidência científica disponível na prestação de serviços efetivos, tanto em termos de resultados clínicos, como no uso dos recursos financeiros, entre outros.

- *Comunidade – o IPO-Porto reconhece que é mais do que um prestador de cuidados hospitalares, é um consumidor de recursos, um criador de lixo, confiando na rede local de transportes. O Instituto é um grande empregador, pelo que é um parceiro significativa na economia local. Refletirá as responsabilidades comunitárias nas decisões que tomar, trabalhando em parceria com a comunidade, os voluntários e outras organizações, de forma a contribuir de forma efetiva nas vidas das pessoas locais e a minimizar o impacto no ambiente.”.[IPO Porto, 2015b]*

O plano estratégico do IPO-Porto está descrito no triângulo estratégico, Figura 1 - Triângulo estratégico do IPO-Porto [IPO Porto, 2015c], e tem como objetivos estratégicos:

- Melhoria da Qualidade dos Serviços;
- Melhoria da Qualidade Percebida;
- Aumento da Sustentabilidade Financeira. [IPO Porto, 2015b]

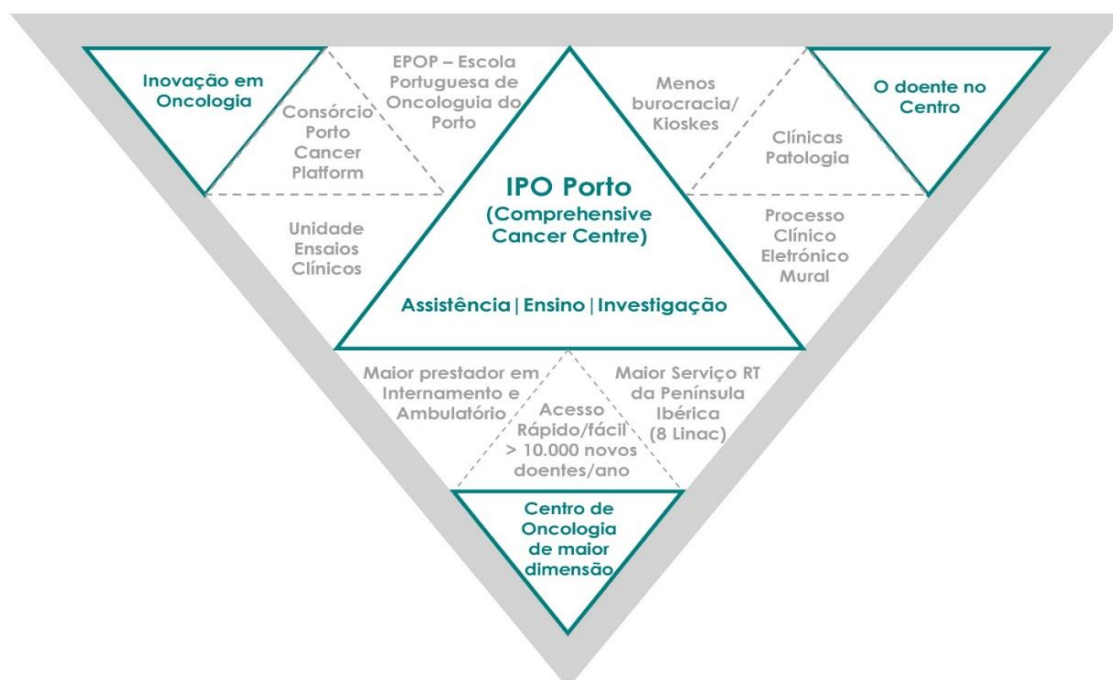


Figura 1 - Triângulo estratégico do IPO-Porto

1.4 Contributos deste trabalho

A implementação do sistema de monitorização e alarmística trouxe grandes vantagens para o serviço de informática, que por sua vez auxiliaram o IPO Porto na sua procura por melhorar a qualidade dos serviços que disponibiliza.

Os resultados provenientes da escolha de uma solução de referência, estudada ao pormenor de modo a garantir que todos os objetivos traçados fossem atingidos, permitindo ao mesmo tempo uma futura expansão. Este sistema capacitou o serviço de informática com um conjunto de ganhos e mais-valias, como:

- Registo de incidentes;
- Ataque focado ao problema;
- Descobrimto das causas do problema;
- Auditoria e inventário;
- Alocação de recursos, tanto humanos como físicos para outras funções;
- Aumento de segurança na privacidade da informação.

1.5 Estruturação do relatório

Este documento está estruturado em cinco capítulos principais, cada um focando uma fase no desenvolvimento do projeto e seguindo uma lógica sequencial.

Introdução

Capítulo introdutório do projeto onde é feita uma breve descrição da organização, onde se enquadra o projeto apresentando os contribuídos que este ofereceu.

Contexto

Apresentação do problema que o projeto se propõe resolver, onde é descrito o estado da arte de soluções presente no mercado e uma visão geral da opção selecionada como melhor escolha.

Ambiente de trabalho

Apresentação dos métodos de trabalho dentro do serviço de informática, onde está inserido a realização deste projeto, descrição do planeamento de todo o trabalho e tecnologias utilizadas.

Descrição técnica

Exposições de todas as fases que compõem o projeto, com maior pormenor na descrição de todos os passos das tarefas e testes realizados e conclusões que levaram às fases seguintes e implementação de novo trabalho.

Conclusões

Finalmente no capítulo final é apresentado um sumário da solução assim como as capacidades/funcionalidades atingidas e limitações detetadas. Apresenta também uma definição de ideias para trabalho futuro.

2 Contexto

2.1 Problema

No serviço de informática do IPO Porto está implementado um sistema de monitorização e alarmística que permite saber em primeira mão o acontecimento de eventos. Estes podem ser classificados em vários níveis de gravidade, desde informativos, avisos e problemas graves, muito graves ou catastróficos, sendo estes possíveis de ser escalonáveis mediante certas condições, como por exemplo, a persistência de certo erro num período de tempo ou a falha de vários serviços num determinado servidor.

A existência deste sistema permite que a equipa do serviço possa rapidamente ser avisada da ocorrência de tais problemas e atuar, de forma atempada e rápida, sobre esses problemas, de modo a mitigar/eliminar possíveis problemas de maior gravidade. Este sistema permite também, praticamente eliminar a necessidade do utilizador final ter que reportar esses problemas, e se a resposta da parte de equipa for rápida o suficiente, até passar completamente despercebido por parte desses mesmos utilizadores.

Este sistema apesar de ser muito prático e útil para o serviço de informática, restringia-se apenas aos vários servidores e serviços existentes no *Datacenter* da instituição. O que acontecia muitas vezes era que se verificava não existirem problemas de maior relevo com os serviços, no entanto o utilizador final reportava muitas vezes problemas com os mesmos. Ora se os servidores estão a funcionar em pleno e mesmo assim observa-se a existência de problemas, qual poderá ser a causa desses problemas? Duas possibilidades são postas sobre a mesa:

- Problemas com o equipamento do utilizador;
- Problema de comunicação entre o servidor e o equipamento;

Se o problema residir no equipamento do utilizador, então um técnico desloca-se ao local para uma análise de modo a identificar qual o problema, e corrige-o se este poder ser resolvido no momento ou efetua uma recolha do equipamento para reparação e eventualmente à troca de equipamento.

Se o problema for de comunicação com o servidor, então é necessário descobrir em que ponto da rede esse problema se encontra. A ligação entre o ponto inicial (equipamento do utilizador)

e o ponto final (servidor) tem que ser analisada, ligação essa que pode passar por três a quatro equipamentos desde o ponto inicial até ao final. Na ligação podem-se encontrar inúmeros problemas quer físicos (cabos desligados/defeituosos ou falha de portas do *switch*) quer administrativos (porta do *switch* desligada ou bloqueios da máquina a rede).

Existe um sistema implementado no serviço de Informática que permite analisar possíveis problemas com os equipamentos de rede e que permite descobrir qual a fonte do problema. Apesar da existência deste sistema, o mesmo apresenta muitas lacunas quer a nível de disponibilidade, quer a nível de deteção/resolução. A solução escolhida para a criação deste sistema é um *software* comercial que, apesar de ter uma componente gratuita, trata-se de uma componente passiva, que funciona mais como uma demonstração do produto para a versão comercial. Versão esta que permite apenas introduzir os equipamentos de rede para análise e mostra apenas um pequeno número de elementos que não são passíveis de ser escolhidos/alterados, representando uma limitação/imposição de funcionalidades. Outra lacuna do sistema é que apenas esta disponível a um elemento da equipa, que na sua ausência do serviço, este tenha que ser notificado para voltar de modo a que este elemento possa aceder ao sistema e possa visualizar qual e onde se encontra o problema, para assim poder dar seguimento à resolução do mesmo.

O objetivo principal será adicionar, ao sistema já existente de monitorização e alarmística, os vários equipamentos de rede e suporte da mesma, configurando uma nova componente dedicada apenas a infraestrutura de rede da instituição, criando conjuntos de elementos importantes e relevantes a serem monitorizados, que permitam uma análise, construção de regras e ações a serem tomadas pelo sistema permitindo assim uma maior disponibilidade para toda a equipa, face ao sistema individual, permitindo assim uma maior disponibilidade e diminuindo o tempo de resposta.

2.2 Áreas de negócio

A área de negócio da saúde engloba um vasto conjunto de áreas de ação, desde cuidados básicos até a áreas de doenças específicas. Estas áreas de ação podem ser acedidas através de serviços geral, hospitais e clinicas gerais, ou em serviços especializados. A área de oncologia é onde o IPO Porto se insere, sendo especializado em todo o tipo de doenças oncológicas assim como o estudo de combate contra o cancro.

Foi em Abril de 1974 que o IPO Porto iniciou as suas funções, e tem-se vindo a distinguir ao longo dos anos pela sua dinâmica e qualidade com que acolhe e trata os doentes, pela atividade científica que desenvolve e pela qualidade do ensino que realiza na área da oncologia. É uma instituição de referência nacional e internacional, sendo membro ativo da *European Organization of Research and Treatment of Cancer* (EORTC). Atualmente o IPO Porto presta assistência a mais de 3,7 milhões de habitantes, da zona de influência da ARS Norte bem como a sub-região de Aveiro-Norte.

2.3 Estado da arte

A área de gestão de redes é bastante rica em plataformas de monitorização e gestão. As próprias marcas de equipamento de rede oferecem soluções para a monitorização dos seus equipamentos. A questão que se levanta é a de procurar qual a melhor solução que se proponha a fazer o que é definido como importante e relevante e ao mesmo tempo que se adapte ao que é desejado sendo por sua vez de simples configuração e utilização.

2.3.1 Nagios

O *Nagios* é uma ferramenta *open source* distribuída através de uma licença GPL, criada por Ethan Galstad. No início dos anos 90 tinha como nome *NetSaint* e começou por ser uma simples ferramenta de DOS que basicamente utilizava o *software utility "ping"* que permitia testar a conectividade com servidores Novell. Outras funcionalidades do *NetSaint* passavam pela recuperação de dados perdidos, guardando-os em ficheiros de texto, e na utilização de aplicações terceiras. Foi assim que nasceu a arquitetura *Server-Plugins* que é a base de funcionamento do *Nagios* donde resultou o seu grande sucesso entre a comunidade. No ano de 1998 o *NetSaint* recebeu uma nova versão que permitiu usar-se em plataformas *Linux*. Esta nova versão foi otimizada, permitindo monitorizar *hosts* e serviços de uma forma mais eficiente. Em 2002 Ethan vê-se obrigado a alterar o nome da sua ferramenta, por questões de *copyright*, e passa então a chamar-se *Nagios*, nome que se vem mantido até aos dias de hoje e com o qual tem vindo a ganhar vários prémios e consequentemente tem vindo a ser cada vez mais utilizado a nível mundial, contando também com uma grande comunidade. [Nagios, 2015a]

2.3.1.1 Funcionamento

O *Nagios* baseia-se numa infraestrutura *Server-Plugins*, ou seja, não permite ao servidor executar tarefas de pedidos e verificações, delegando esse trabalho a componentes externos (*plugins*) disponíveis, que ficaram então encarregues de realizar esses pedidos e verificações, Figura 2 - Exemplo de funcionamento de um *plugin*. A extrema flexibilidade do *Nagios* reside na possibilidade de integrar esses *plugins*, independentemente da fonte e linguagem utilizada para a sua criação.

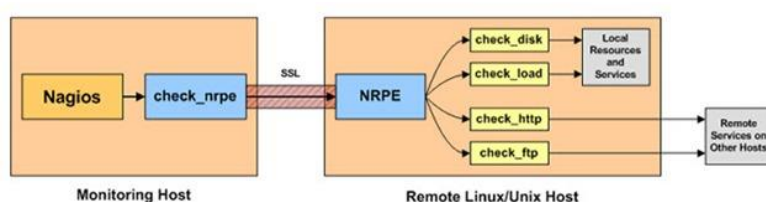


Figura 2 - Exemplo de funcionamento de um *plugin* [Pplware, 2015a]

O *Nagios* divide os vários objetos passíveis de serem monitorizados em duas grande categorias. A primeira categoria é o onde estão inseridos todos os equipamentos físicos tais como servidores, impressoras, *switchs* e *UPS* e designa-se por *Hosts*. Na segunda categoria estão inseridos todos os serviços e funcionalidades dos *hosts*, desde serviços de correio eletrónico, páginas *web*, *webservices*, *printservers* até administração de rede designa-se por *Services*. É possível a criação de um conjunto de *hosts* e também é possível associar a um *host* um conjunto de *services*, permitindo assim um melhor controlo e organização sobre a estrutura.

Os *plugins* recolhem a informação e passam-na ao servidor, que então analisa essa informação e a converte para a interface *web* com os vários estados dos objetos.

A informação é apresentada através de uma interface *web* que não se limita a apresentar números e percentagens no ecrã, que podem ser confusos e mal interpretados, mas sim num sistema de cores e níveis de gravidade que podem ser personalizados em função do objeto monitorizado, Figura 3 - Interface *web* do *Nagios*. Esses níveis e cores revela de uma forma rápida o seu estado e passam de “OK” sem problemas, “WARNING” valores fora do normal, “CRITICAL” problema e “UNKOWN” sem informação. [Nagios, 2015b]

HOSTS

Host	Service	Status	Last Check	Duration	Attempt	Status Information
OC-Example	absentExample	UNKNOWN	09-12-2007 09:35:53	1d 0h 57m 55s	3/3	STATE_UNKNOWN: dummy not found
	aExample	WARNING	09-12-2007 09:36:22	0d 0h 4m 17s	3/3	STATE_WARNING: adosHost:aExample in MINOR severity status: 1e: 0 sec.
	aExample1	WARNING	09-12-2007 09:36:52	0d 0h 3m 47s	3/3	STATE_WARNING: adosHost:aExample1 in MINOR severity status: 1e: 0 sec.
	aExample2	WARNING	09-12-2007 09:37:21	0d 0h 39m 25s	3/3	STATE_WARNING: adosHost:aExample2 in MINOR severity status: 1e: 2 sec.
	aExample3	OK	09-12-2007 09:34:50	0d 0h 8m 37s	1/3	STATE_OK: adosHost:aExample3 5 2007-09-12 09:34:48.285348 : 1e: 2 sec.
	cokExample	OK	09-12-2007 09:35:20	0d 0h 2m 19s	1/3	STATE_OK: adosHost:cokExample 5 2007-09-12 09:35:19.823430 : 1e: 1 sec.
	cokExample1	WARNING	09-12-2007 09:35:49	0d 0h 9m 38s	3/3	STATE_WARNING: adosHost:cokExample1 in MINOR severity status: 1e: 1 sec.
	cokExample2	OK	09-12-2007 09:36:18	0d 0h 1m 21s	1/3	STATE_OK: adosHost:cokExample2 5 2007-09-12 09:36:17.410902 : 1e: 1 sec.
	cokExample3	CRITICAL	09-12-2007 09:37:08	0d 0h 1m 31s	2/3	STATUS_CRITICAL: adosHost:cokExample3 in MAJOR severity status: 1e: 5 sec.
	compressExample	OK	09-12-2007 09:36:37	0d 1h 18m 40s	1/3	STATE_OK: adosHost:compressExample 10 2007-09-12 09:36:37.048426 3 : 1e: 0 sec.
LivePICS	Current Load	OK	09-12-2007 09:34:06	0d 0h 14m 21s	1/4	OK - load average: 0.19, 0.15, 0.10
	Current Users	OK	09-12-2007 09:34:36	0d 0h 13m 51s	1/4	USERS OK - 5 users currently logged in
	PING	OK	09-12-2007 09:35:05	0d 0h 13m 22s	1/4	PING OK - Packet loss = 0%; RTA = 0.11 ms
	Root Partition	OK	09-12-2007 09:35:34	0d 0h 12m 53s	1/4	DISK OK - free space: / 4105 MB (44% inode=95%):
	Total Processes	OK	09-12-2007 09:36:04	0d 0h 12m 23s	1/4	PROCS OK: 39 processes with STATE = RSDZT

Figura 3 - Interface web do Nagios

2.3.1.2 Pontos fortes

- Solução *open source*;
- Monitorização intrusiva e não intrusiva;
- Monitorização de servidores (Windows / *Unix), serviços e equipamentos ativos da rede;
- Possibilidade de desenvolvimento, de *plugins* específicos às necessidades de cada administrador;
- Possibilidade de definir a monitorização da rede de forma hierárquica;
- Escalável, uma vez que os processos de monitorização são executados de forma paralela;
- Capacidade de distribuir a monitorização por vários servidores *Nagios*;
- Notificação para quando é detetado um problema e para quando o mesmo é considerado resolvido;
- Capacidade de executar ações de resolução sobre os problemas quando estes são detetados;
- Grande comunidade e repositório de *plugins*;

2.3.1.3 Pontos fracos

- Completa dependência de *plugins*;
- Apenas executa em ambiente *Linux*;
- Exige um alto nível de *know how* para efetuar configurações básicas;
- Falta de uma ferramenta gráfica para configuração da plataforma;
- Interface gráfica bastante técnica e pouco simplificada;
- Falta de *dashboards* editáveis de alta qualidade para representação de elementos de negócios;
- Carência de relatórios mais complexos sobre disponibilidade, planeamento de capacidades e *SLAs*;
- Nativamente não é possível criação de histórico da informação;
- Falta de um mecanismo de *autodiscovery* de elementos de rede;
- Falta de aderência às melhores práticas de gestão de TI, como o ITIL;
- Falta de suporte à interface multilinguagem;

2.3.2 Cacti

O Cacti é uma interface completa escrita em *PHP* para a plataforma *RRDTool* e que armazena os dados numa base de dados *MySQL* que cria e apresenta um conjunto de gráficos dos dados recolhidos. Foi criado por Ian Berry, que quando trabalhava para um *ISP* americano, deparava-se com um problema comum de dificuldades na utilização do *RRDTool* devida a sua complexidade e a um interface pouco *user friendly*. No ano de 2001 teve a ideia de aliar as funcionalidades de armazenar e gerar gráficos do *RRDTool* com o *Net-SNMP*, que utiliza o protocolo *SNMP* para efetuar recolha de dados, armazenando esses dados numa base de dados *MySQL* e criar uma interface mais simples e intuitiva para o utilizador, escrita em *PHP*. Nasce assim o *Cacti* que com o seu sucesso tem visto a equipa de desenvolvimento crescer assim como da sua comunidade espalhada pelo mundo. [Wikipedia, 2015a]

2.3.2.1 Funcionamento

O Cacti baseia-se num conjunto de três tarefas, cada uma utilizando uma ferramenta diferente, para monitorizar os objetos desejados.

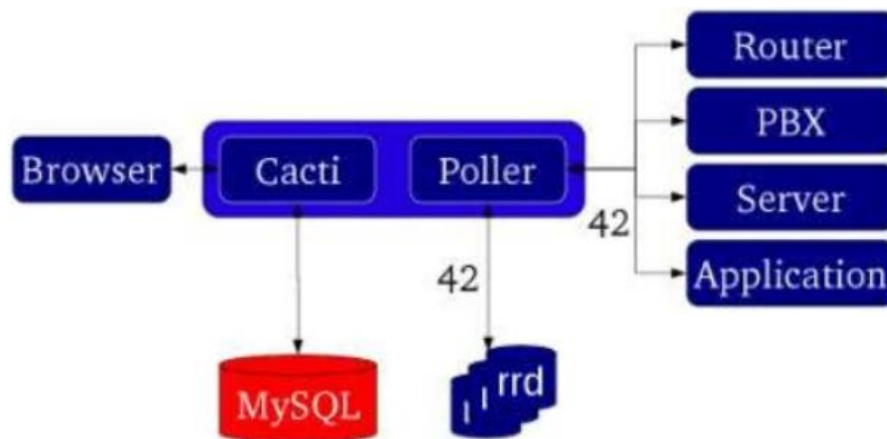


Figura 4 - Princípio de funcionamento base do Cacti

A primeira tarefa é a recolha de dados dos diferentes objetos. Utilizando um *poller*, que é uma aplicação que periodicamente vai efetuar a recolha de dados definido pelo administrador, recaindo esse trabalho na aplicação *Net-SNMP* que utiliza o protocolo *SNMP* para realizar a recolha remotamente, Figura 4 - Princípio de funcionamento base do Cacti. Todos os equipamentos que tenham funcionalidade *SNMP* são passíveis de ser monitorizados pelo *Cacti*. A segunda tarefa é o armazenamento dos dados onde cabe ao *core* do *Cacti*, o *RRDTool*, que recorre a padrões *RRD* para consolidar a informação recolhida, através de funções como o *AVG*, *MIN*, *MAX* entre outras, evitando assim que a base de dados, em *MySQL*, vá crescendo de tamanho eliminando o trabalho constante de aumento/limpeza da mesma. A tarefa final é disponibilizar a informação. O *Cacti* permite ao administrador gerar relatórios e gráficos com os dados recolhidos e armazenados permitindo assim uma melhor análise do funcionamento dos vários equipamentos. A criação desses gráficos é facilitada pois contém uma área de seleção que permite a customização, dando a possibilidade de amostragem de um único item ou um conjunto de itens, com varias cores e formatos, introdução de campos e legendas recorrendo também a *templates*, Figura 5 - Interface gráfica do Cacti [Cacti, 2015]. [Cacti, 2015]

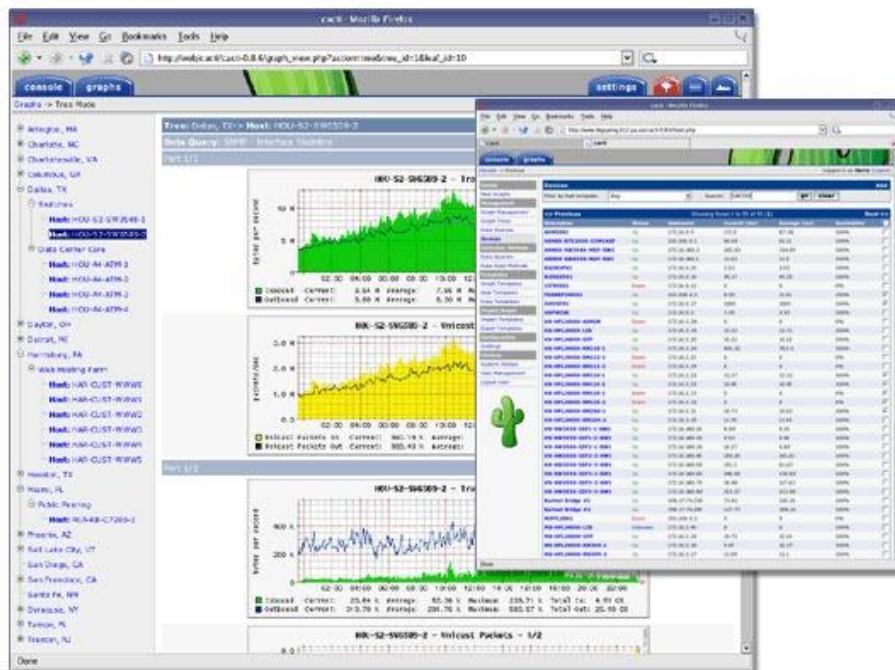


Figura 5 - Interface gráfica do Cacti [Cacti, 2015]

2.3.2.2 Pontos fortes

- Solução *open source*;
- Bastante rápido não exigindo um grande poder de processamento;
- Execução em ambientes *Linux* e *Windows*;
- Permite a introdução de *plugins*;
- Configuração bastante acessível;
- Interface gráfica simples e limpa;
- Gráficos gerados com vários níveis de customização;
- Os registros do *RRDtool* armazenados nos arquivos *“.rrd”* mantêm o mesmo tamanho e não aumentam;

2.3.2.3 Pontos fracos

- Nativamente apenas permite monitorizar equipamentos com funcionalidades *SNMP*;
- Apenas permite monitorização, sem funcionalidade de alarmística;
- Falta de um mecanismo de *autodiscovery* de elementos de rede;
- Instalação individual dos vários elementos necessários;

- Exige a introdução manual de todos os equipamentos a monitorizar;
- Apenas monitoriza equipamento físico, não contempla serviços;

2.3.3 SpiceWorks

Foi fundado em Janeiro de 2006 por um grupo de 4 pessoas, Scott Abel, Jay Hallberg, Greg Kattawar e Francis Sullivan que tinham como intuito criar um software de gestão de TI que iria apoiar todos os profissionais de TI espalhados pelo mundo. A meio do ano de 2006 lançaram uma versão beta, que teve uma excelente aceitação por parte de comunidade, sendo lançada a versão 1.0 em Novembro de 2006, tendo no fim desse ano um total de 120,000 utilizadores. Desde 2006 a comunidade tem vindo a crescer e a tornar cada vez mais esta aplicação mais robusta e fiável. Esse apoio tem permitido a evolução do software, o que tem levado ao lançamento de novas versões com mais funcionalidades. [Wikipedia, 2015b]

De notar que é uma aplicação gratuita, mas que contem vários elementos de publicidade que para sua remoção exige o pagamento de um valor.

2.3.3.1 Funcionamento

O SpiceWorks IT Desktop é uma ferramenta composta por vários módulos cada um pensado para uma função específica.

O módulo de inventários de rede (Inventory Management), Figura 6 - Módulo de Inventário [SpiceWorks, 2015], permite ao administrador catalogar todo o hardware existente no seu parque informático. Tem embebido a funcionalidade de fazer uma pesquisa pela rede indo recolhendo todo e qualquer equipamento que tenha um endereço IP associado, desde computadores/servidores Windows, Mac, e Linux, unidades de armazenamento, switch e routers, ups e permite controlar dispositivos fora da rede. Neste módulo é possível também criar listas de todo o *software* instalado num determinado dispositivo ou efetuar um rastreio completo de todas as licenças de software assim como descobrir, monitorar e gerir serviços de *cloud* na rede até mesmo os que não são reportados pelos utilizadores. Tem também embebido uma funcionalidade de criação de relatórios dos todos os ativos da rede possuindo dezenas de relatórios internos e milhares de partilhados pela comunidade. [SpiceWorks, 2015]



Figura 6 - Módulo de Inventário [SpiceWorks, 2015]

Com o módulo de monitorização da rede (Network Monitoring) o administrador de Sistemas tem ao seu dispor uma ferramenta que lhe permite saber, em tempo real, o estado da sua rede e dos equipamentos ativos que a constituem, Figura 7 - Interface gráfica do *Spiceworks* [SpiceWorks, 2015]. Mantendo o controlo do desempenho dos, por exemplo de, servidores e tempos de atividade podem ser monitorizados se algum equipamento esta a ter um comportamento anormal. Este módulo permite também que o administrador possa ficar informado de softwares instalados e por qual utilizador podendo aceder aos *logs* e eventos dos equipamentos da rede. A nível de rede física permite analisar a saturação da rede e largura de banda podendo localizar possíveis *bottlenecks* e outros pontos de problemas.

Existe também um módulo de gestão de pedidos e de *Help Desk*, que permite registar ocorrências de problemas, atribuir a equipa para resolução dos mesmos e notificando o utilizador do estado. Nos dias de hoje este módulo é considerado como um elemento essencial para o administrador de redes/sistema. [SpiceWorks, 2015]

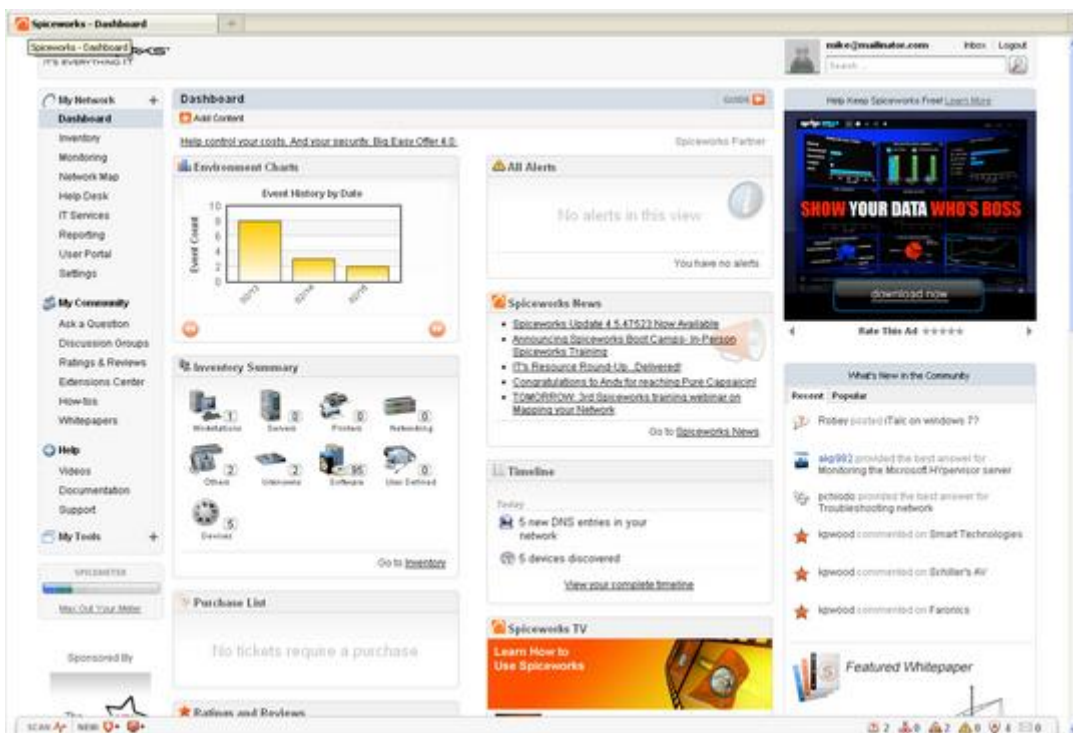


Figura 7 - Interface gráfica do Spiceworks [SpiceWorks, 2015]

2.3.3.2 Pontos fortes

- Aplicação completamente gratuita;
- Dimensão da comunidade;
- Constante evolução;
- Conjuga varias ferramentas de administração/monitorização de sistemas e redes uma só solução;
- Extensível com outros produtos;
- Intuitiva e de fácil utilização/compreensão;
- Baixa curvatura de aprendizagem.

2.3.3.3 Pontos fracos

- Só é suportado em sistemas *Windows*;
- Publicidade pode torna-se incomodativa e usa a informação do utilizador para a direcionar;
- Baixa performance em redes de grande dimensão;
- Escalabilidade reduzida;

- Limitações na deteção de equipamento com sistemas operativos não Windows;
- Não permite um nível de profundidade de monitorização e controlo, que outras soluções apresentam;
- Requer configurações iniciais nos equipamentos de modo a serem reconhecidas pelo Spicework.

2.3.4 Observium

Ao longo do tempo o Observium foi designado por vários nomes. Em 2006 Adam Armstrong iniciou o projeto *Project Observer*. Mais tarde em 2008 adotou o nome de *ObserverNMS* até 2010 onde teve a designação final. Este projeto foi crescendo com intuito de colmatar uma lacuna existente, que é falta de um sistema *NMSes* de fácil utilização. Destina-se a fornecer ao administrador de sistemas uma interface mais "*user-frindelly*" que permita observar a performance e saúde da sua rede. Os seus objetivos principais baseiam-se na coleta do máximo possível de informação do histórico dos equipamentos, sendo este completamente autónomo no descobrimento dos mesmos, com pouca ou nenhuma intervenção tendo contudo uma interface intuitiva. Este foi pensado principalmente para redes Cisco e Linux, mas não se baseia apenas nessas arquiteturas oferecendo suporte a uma ampla gama de ativos de rede e de sistemas operativos. [Wikipedia, 2015c]

2.3.4.1 Funcionamento

Fortemente enraizada na aplicação, a plataforma *RRDtool* utiliza o protocolo SNMP para recolher informações dos equipamentos, o que lhe permite a ter a capacidade incrível de auto reconhecimento total de toda a rede, isto com pouca ou nenhuma intervenção humana, criando assim um inventário exato. Graças a essa funcionalidade o Observium suporta uma grande variedade de sistemas operativos e equipamentos, tais como *Linux, Windows, FreeBSD, Cisco, HP, Dell, NetApp, Juniper, Brocade, Foundry* e muitos mais.

Tendo por base uma infraestrutura *PHP/MySQL* apresenta uma interface gráfica robusta, Figura 8 - Interface gráfica do Observium[Observium, 2015], mas ao mesmo tempo simples que permite passar ao administrador toda a informação recolhida através de um conjunto de gráficos padronizáveis, gráficos esses que lhe permitirão analisar a saúde e performance da rede. A recolha de dados é a um nível massivo, recolhendo tudo o que é passível de ser recolhido de determinado equipamento.

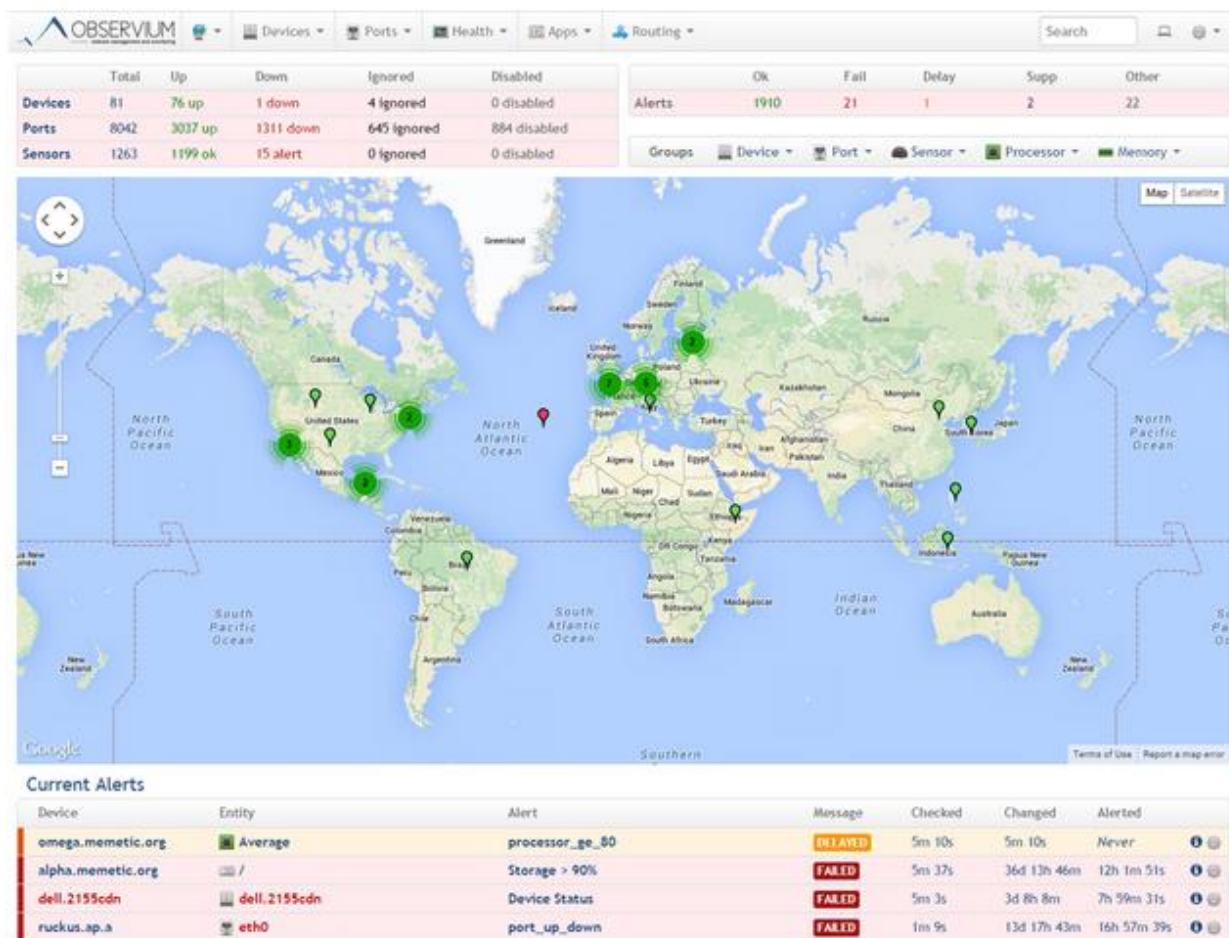


Figura 8 - Interface gráfica do Observium[Observium, 2015]

Sendo este o *core* de funcionamento do Observium, o controlo sobre a recolha é nulo não permitindo selecionar que dados são relevantes ou não sobre determinado equipamento, tendo apenas a escolha o alcance de tempo que os gráficos são apresentados, Figura 9 - Dados recolhidos pelo Observium [Observium, 2015]. Esta recolha massiva acarta problemas de latência que devem ser bem ponderados e estudos antes da implementação desta solução.

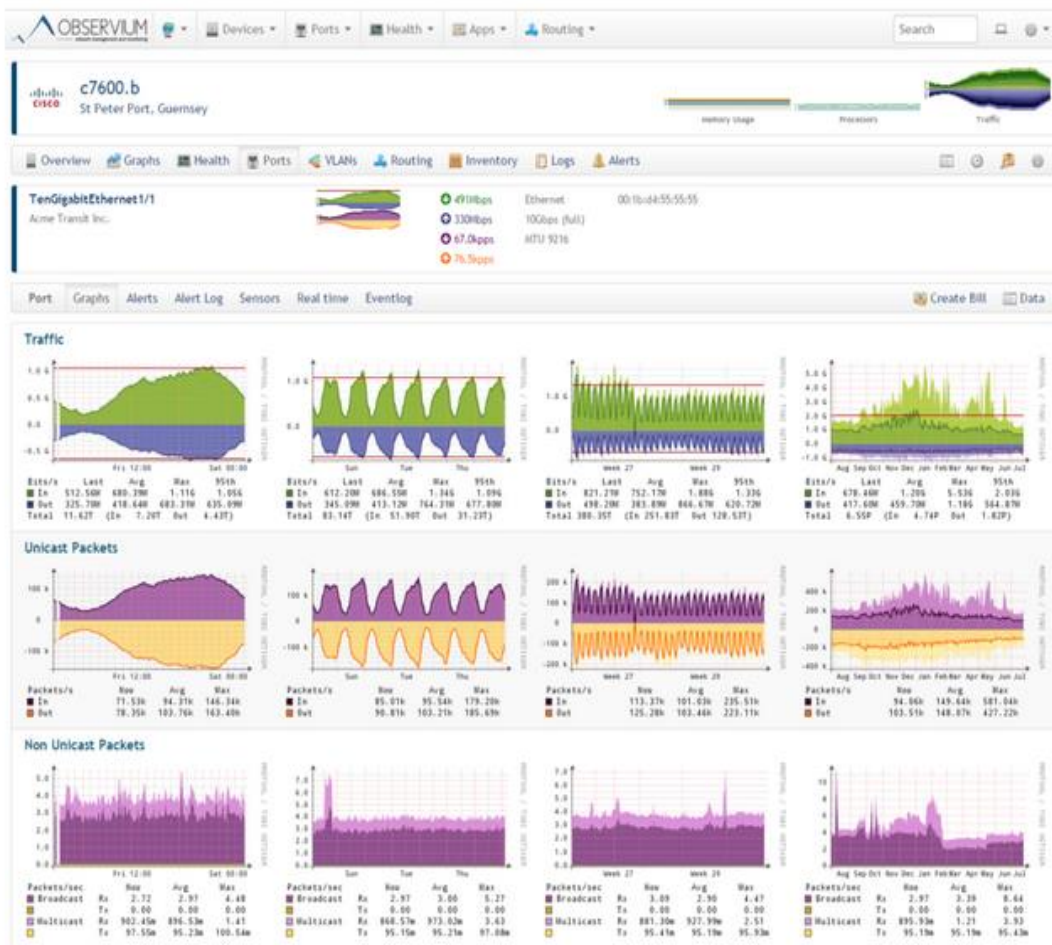


Figura 9 - Dados recolhidos pelo Observium [Observium, 2015]

Na versão gratuita de Observium não apresenta qualquer tipo de alarmística nativa, sendo necessário o uso de outro tipo de aplicação para esse efeito.

2.3.4.2 Pontos fortes

- Aplicação completamente gratuita;
- Suporte a um enorme número de sistemas operativos/hardware;
- Autodescoberta de equipamentos;
- Intuitiva e de fácil instalação/utilização/compreensão;
- Trafego em tempo real.

2.3.4.3 Pontos fracos

- Sem sistema de alarmística;

- Apenas baseado em SNMP;
- Não possibilidade de monitorização de serviços em portas;
- Pode causar baixa performance em redes de grande dimensão;
- Impossibilidade de configuração da informação a recolher/apresentar.

2.3.5 Zabbix

O Zabbix começou por ser um projeto interno, desenvolvido por Alexei Vlashev em 1998. Mais tarde, 2001, é lançada a primeira versão não estável do Zabbix sobre uma licença GPL. Esta versão foi sendo corrigida e melhorada e em 2004 sai a sua primeira versão estável (v.1.0). No ano de 2005 é fundada a companhia Zabbix SIA que começa a fornecer suporte técnico e comercial do produto. Mais recentemente abre em 2012 a Zabbix Japão LLC, continuando assim o seu crescimento incluído cada vez mais funcionalidades e potencialidade. [Wikipedia, 2015d]

É um software de monitorização distribuído e Open Source, considerado por muitos como uma das melhores ferramentas de monitorização da atualidade, devido ao conjunto de funcionalidades que disponibiliza, a simplicidade do seu *frontend*, Figura 10 - Interface Web do Zabbix, em questões como a instalação, configuração, manutenção e gestão de todos os seus componentes e suporte a uma inúmera quantidade de tecnologias tais como SNMP v1,v2,v3 , IPMI , JMX, SSH, Agentes, *VMware*, Bases de Dados, Sites e muito mais.

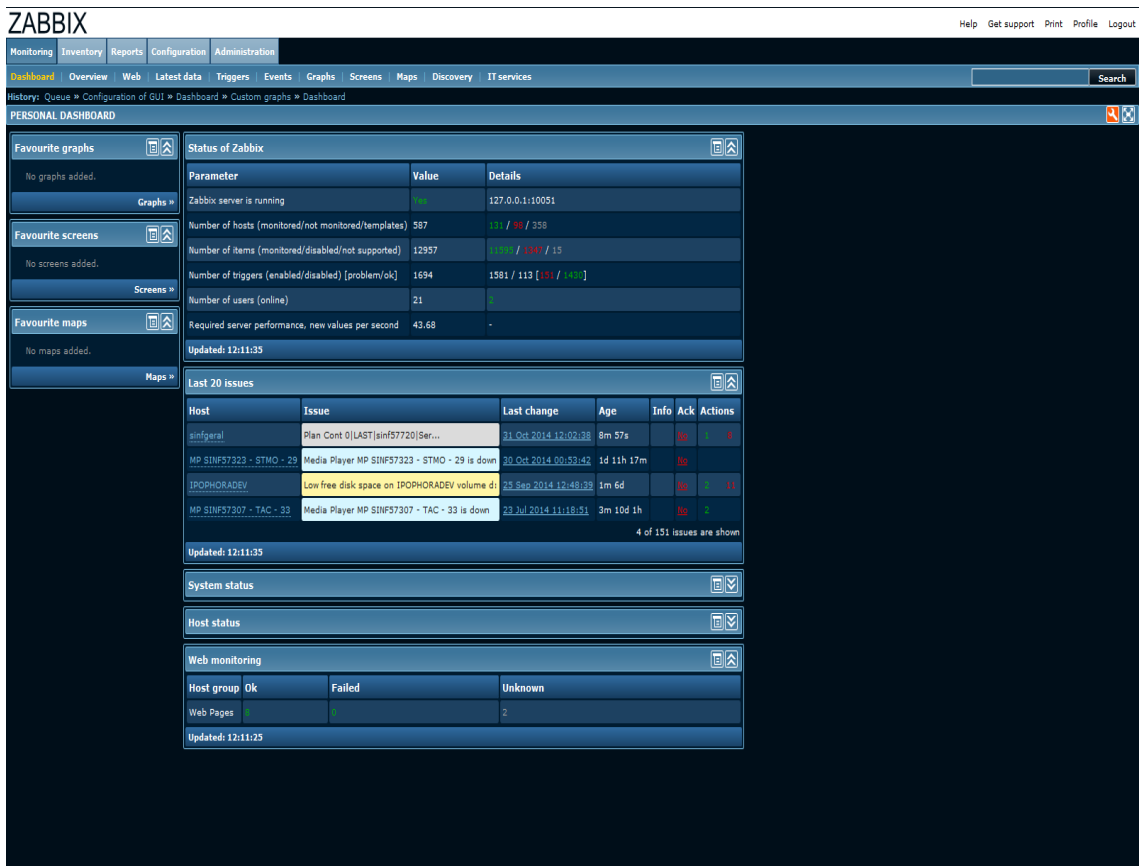


Figura 10 - Interface Web do Zabbix

2.3.5.1 Funcionamento

Na sua composição estão presentes vários elementos permitindo assim de antemão, planejar como será a sua estrutura. A base da estrutura do Zabbix passa por três componentes essenciais, um servidor Zabbix, uma base de dados e a interface Web.

O servidor Zabbix é o elemento central e é responsável pela recolha e armazenamento de todos os dados monitorizados, basicamente é um repositório central de dados, Figura 11 - Principio de funcionamento base do Zabbix [Pplware, 2015b]. Essa recolha pode ser efetuada por ele próprio ou com o auxílio de agentes e *proxies*. Cabe-lhe também a tarefa de criar gráficos e mapas, assim como cálculo e o despoletar de *triggers* e executar as ações a eles inerentes, desde envio de notificações como execuções a scripts. Apesar de disponibilizar agentes aos mais diversos sistemas operativos o servidor tem que estar hospedado numa máquina com Linux ou Mac OS. Outro elemento chave é a base de dados onde serão armazenadas todas as configurações do Zabbix assim como de toda a informação recolhida. Toda a recolha de informação é centralizada numa única interface Web, 100% online, que permite a consulta/análise dos dados, assim como

a criação de todas as configurações. Este permite a criação de perfis de utilizadores e atribuir acessos e quais ações este podem executar. Um elemento que, não sendo central, traz um leque de opções que permite por um lado diminuir a carga do servidor, descentralizando a recolha num único ponto mitigando assim *bottlenecks* por outro permitir a monitorização de ambientes remotos, é o Zabbix proxy. Os agentes da *proxies* enviam os dados para o Zabbix proxy que por sua vez reencaminha para o Zabbix server sendo assim necessário utilizar apenas um porto de comunicação evitando assim grandes configurações nas *firewalls* implementadas. Este sistema previne perda de informação pois mesmo que a ligação servidor-proxy se perca, a *proxy* continuara a recolher informação, passando-a quando a ligação for reestabelecida. Outra opção são os agentes Zabbix correm nas maquinas a monitorizar funcionado como um *daemon* ou serviço, e são responsáveis por enviar todas as informações requisitadas pelo servidor/proxy. [Zabbix, 2015]



Figura 11 - Princípio de funcionamento base do Zabbix [Pplware, 2015b]

2.3.5.2 Pontos fortes

- Licença Open Source;
- Interface Web 100% *online*;

- Fácil instalação e customização;
- Solução distribuída;
- Autodescoberta de equipamentos;
- Grande variedade de *templates* pré-definidos;
- Criação de gráficos em tempo real.






2.3.5.3 Pontos fracos

- Curva de aprendizagem alta;
- Necessita de um bom planejamento para ambientes de grandes dimensões;
- Grande consumidor de recursos.

Depois de analisadas todas as capacidades e funcionalidades das várias aplicações acima apresentadas foi possível criar uma tabela, Tabela 1 - Comparativo de Soluções, onde é possível efetuar uma análise frente-a-frente, que permite uma escolha mais consciente e acertada, tendo em conta o que é necessário configurar para o cenário em questão.

Pode-se observar que existem alguns pontos em comum entre as aplicações, mas os pontos não contemplados por umas aplicações, permitem ser um ponto de decisão sobre essa solução em detrimento das outras aplicações. Essa escolha está sempre condicionada ao objetivo final do projeto assim como dos recursos.

Tabela 1 - Comparativo de Soluções

Nome da Solução	 CACTI	 Nagios®	 OBSERVIVUM <small>— observ management and networking</small>	 SPICEWORKS	 ZABBIX
Relatórios IP SLA	Sim	Via plugin	Sim	Sim	Sim
Grupos Lógicos	Sim	Sim	Sim	Não	Sim
Tendências	Sim	Sim	Sim	Sim	Sim
Previsão de Tendências	Sim	Não	Não	Não	Não
Auto Descobrimto	Via plugin	Via plugin	Sim	Sim	Sim
Agentless	Sim	Suportado	Suportado	Sim	Suportado
SNMP	Sim	Via plugin	Sim	Sim	Sim
Syslog	Sim	Via plugin	Sim	Sim	Sim
Plugins	Sim	Sim	Sim	Sim	Sim
Triggers / Alertas	Sim	Sim	Sim	Sim	Sim
WebApp	Controlo Total	Controlo Total	Sim	Sim	Controlo Total
Monitoração Distribuída	Sim	Sim	Não	Não	Sim
Inventario	Sim	Via plugin	Sim	Sim	Sim
Plataforma	PHP	C, PHP	PHP	PHP	C, PHP
Método de Armazenamento de dados	RRDtool MySQL	Flat file SQL	RRDtool MySQL	SQLite	Oracle, MySQL PostgreSQL, IBM DB2, SQLite
Licença	GPL	GPL	QPL Commercial	GPL	GPL
Mapas	Via plugin	Sim	Sim	Não	Sim
Controlo de Acessos	Sim	Sim	Sim	Não	Sim
IPv6	Sim	Sim	Sim	Sim	Sim

Como se pode observar pela Figura 12 - Posicionamento das aplicações, se o objetivo se inclinar mais para a monitorização dos sistemas então o spiceworks e o cacti contem melhores argumentos, enquanto que, se for necessário uma aplicação virada para a supervisão do sistema, a escolha pode tender mais para aplicações como o Observium e o Nagios. Se

quisermos uma aplicação mais global que junta o melhor dos dois mundos, monitorização e supervisão, então Zabbix deve ser tomado em conta na decisão final.



Figura 12 - Posicionamento das aplicações

2.4 Visão da solução

Aquando do início deste projeto, nas reuniões iniciais foram determinadas um conjunto de funcionalidades e características que foram divididas em três níveis, essenciais, relevantes e opcionais. Como essenciais foram agrupadas todas as funcionalidades que a solução tinha que permitir. Neste grupo estavam inseridos as questões de criação de um sistema alarmístico que devesse notificar de diferentes modos os vários elementos da equipa.

Também ficou definido como essenciais questões de monitorização relativas a violações de portas nos routers e switches (acesso não autorizado), e a monitorização de portas chave onde se encontravam equipamentos críticos para o normal funcionamento da instituição e equipamentos que estavam ligados a questões com suporte básico de vida e/ou questões de vida ou morte. Como característica principal tinha de ser um sistema que não envolvesse qualquer custo na aquisição e suporte da solução.

No grupo das funcionalidades relevantes entravam questões de monitorização de equipamentos, elaborar um estudo de possibilidades de monitorização e a partir desse estudo tomar decisões de quais e como deviam ser adicionadas ao plano de monitorização. A

disposição da informação também foi marcado como um ponto relevante, a criação de um *dashboard* onde a informação mais crítica deverá ser apresentada, maior destaque para problemas que estão a acontecer em tempo real, mas também com a apresentação de mapas por edifício e andar de toda a instituição, gráficos de maior relevância e relatórios de estados.

Outra funcionalidade relevante é a possibilidade de serem tomadas ações aquando dos problemas, como a execução de scripts. O auto preenchimento de informação de cada equipamento, criando assim um inventário do que existe na rede assim como as suas características. Característica relevante seria ser possível aceder a aplicação remotamente sem grande necessidade de configurações, permitindo assim ter acesso a informação sem a necessidade de ser necessário de deslocação ao serviço de informática fora do seu horário de funcionamento.

Como opcional e sendo uma ideia a implementar no futuro a integração do sistema de monitorização e alarmística com o sistema OTRS, já implementado de Helpdesk e ticketing, permitindo que questões consideradas não críticas e passíveis de serem resolvidas pelos elementos da equipa de microinformática e/ou por elementos da equipa do serviço de instalações e equipamentos (SIET).

Também como trabalho futuro ficou pensado a criação de um sistema de *Bussiness Intelligence* para analisar todo o histórico da informação recolhida, que permitisse a criação de relatórios e executar auditorias a todo sistema e rede.

No serviço de informática existem já implementados dois sistemas de monitorização, um com a solução *Zabbix*, que estava apenas focado na monitorização do *datacenter* da instituição, e ou outro com *Observium* versão gratuita, que estava virada para a monitorização de rede. Foi feito um levantamento das soluções existentes que permitissem criar o sistema de monitorização e foram postas lado a lado, as características que cada aplicação fornecia com o que era exigido e chegou-se a conclusão que a solução que melhor encaixava com os requisitos, e permitia também uma maior abertura para futuros projectões que venham a auxiliar no bom funcionamento do serviço e da própria instituição, foi o *Zabbix*.

Foi uma escolha mais óbvia pois das apresentadas apresentava as mais-valias sendo uma solução bastante completa e que permite uma configuração mais específica e focalizada, assim

como um maior controlo na disponibilidade da informação. Permitindo ao mesmo tempo um maior equilíbrio entre a monitorização e a supervisão do sistema.

3 Ambiente de trabalho

3.1 Metodologia de trabalho

O serviço de informática está dividido em três áreas, direção, departamento de microinformática composto por sete elementos, e departamento de sistemas, composto por cinco elementos. O departamento de microinformática é a porta de entrada de onde todos os problemas, relativos ao serviço de informática, passam, sendo que passa primeiro por um elemento do departamento, designado de primeira linha, sendo este contacto efetuado via telefone, correio eletrónico ou presencial.

Esse pedido sofre uma triagem. Se este problema estiver dentro das competências do elemento de suporte da primeira linha é então analisado e se possível resolvido. Se o problema se encontrar fora das suas competências é então reencaminhado para os elementos da segunda linha. A segunda linha é onde estão inseridos os restantes membros da equipa e está dividida nos dois departamentos:

- Microinformática - responsável por problemas de hardware e instalação/reinstalações/remoções de software;
- Sistemas – responsável por todos os sistemas da instituição desde Bases de dados, armazenamento, updates/upgrades, rede e envio de relatórios a fornecedores de problemas.

Estes departamentos funcionam em constante interação um com o outro, tentando fornecer o melhor serviço possível a todo o hospital, Figura 13 - Metodologia de trabalho do serviço de informática.

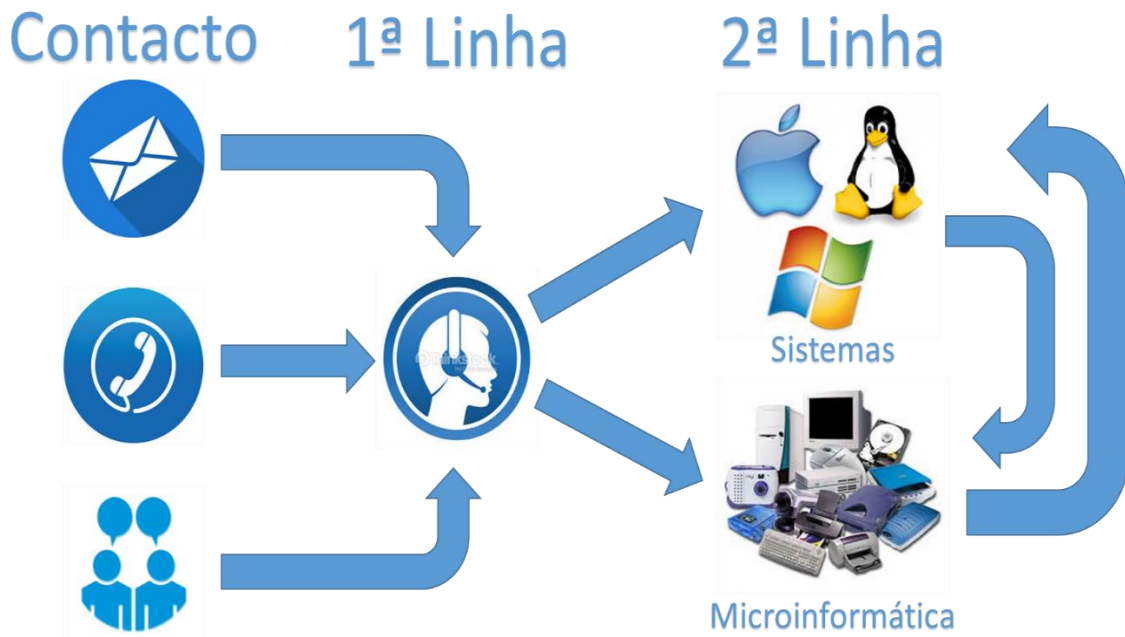


Figura 13 - Metodologia de trabalho do serviço de informática

O projeto da criação do novo sistema de monitorização e alarmística foi inserido no departamento de sistemas, visto que era o departamento que obtinha mais ganhos com a sua criação, não impedindo este facto de o departamento de microinformática poder também interagir com o sistema, analisando a informação e tirando conclusões que lhe permita perceber a causa e resolução dos mesmos, que estejam inserido na sua lista de competências.

Todas as ações tomadas eram precedidas de reuniões onde os objetivos eram definidos. Todos os estudos, configurações e testes foram efetuados em regime flexível, devido ao facto de estarem a ser realizados em ambiente de teste estanque. Foi criada documentação para suportar/auxiliar as várias tomadas de decisão, permitindo assim fundamentar a relevância/não relevância dos itens escolhidos. No final da tarefa, depois de analisada toda a informação recolhida e as configurações efetuadas, foram realizados debates para discutir possíveis correções e modos alternativos de configuração, assim como novas ideias de cenários não contemplados.

3.2 Planeamento de trabalho

No início do projeto, nas primeiras reuniões ficou definido que o projeto ia ser dividido em duas fases, uma fase de desenvolvimento e outra de produção. A primeira fase, Tabela 2 - Mapa de Grant da fase de desenvolvimento, foi estruturada num conjunto de tarefas, que deviam ser cumpridas dentro de um prazo estabelecido, podendo este ser ultrapassado mas ficando definido como derrapagem. Estas tarefas estão interligadas exigindo assim que sejam completas por ordem sequencial.

Tabela 2 - Mapa de Grant da fase de desenvolvimento

Tarefa	Início	Duração (Dias)	Derrapagem
Definição de Requisitos	0	1	0
Instalação de sistema de testes	1	3	0
Estudo de versões	4	5	0
Replicação de sistema (Switch)	9	15	0
Estudo de elementos de alarmística (Switch)	24	3	0
Aplicação de alarmística no sistema de testes (Switch)	27	15	0
Testes do sistema	42	10	0
Replicação de sistema (UPS)	52	15	0
Estudo de elementos de alarmística (UPS)	67	3	0
Aplicação de alarmística no sistema de testes (UPS)	70	15	0
Testes do sistema	85	5	0
Replicação de sistema (AP)	90	15	0
Estudo de elementos de alarmística (AP)	105	3	0
Aplicação de alarmística no sistema de testes (AP)	108	15	0
Testes do sistema	123	5	0
Estudo e aplicação da disposição da informação	128	10	0
Decisão Tecnológica	138	2	0
	Total	140	0

A segunda fase do projeto, a fase de passagem para produção, foi dividida também num conjunto de várias tarefas, Tabela 3 - Mapa de Grant da fase de transição para produção, sendo estas executadas igualmente de uma forma sequencial. Essas tarefas focalizaram-se na importação das configurações e introdução de todos os equipamentos no sistema e na criação do modelo de visualização de toda a informação.

Tabela 3 - Mapa de Grant da fase de transição para produção

Tarefa	Início	Duração (Dias)	Derrapagem
Definição de Nomes	0	1	0
Criação novos hostgroups	1	1	0
Importar Templates	2	2	1
Criação de novos hosts	4	10	0
Criação de mapas	14	10	0
Importar mapas	24	2	0
Criação de screens	26	10	0
Importação de screens	36	2	0
Criação de slide show	38	4	0
Testes do sistema	42	10	0
Decisão Tecnológica	52	2	0
	Total	54	1

3.3 Tecnologias usadas

Durante toda a realização do projeto foram utilizadas diversas ferramentas e tecnologias que permitiram a conclusão do projeto com sucesso. As ferramentas principais foram o sistema operativo de base do Zabbix, Cent OS 6.5, e a aplicação Zabbix em si, versão Zabbix 2.0.3. a elaboração de toda a documentação auxiliar foi realizada com recurso ao Microsoft Office, desde Microsoft Word, Microsoft Excel, Microsoft Power Point e Microsoft Visio. No descobrimento de endereços de IP e outra informação necessária, nomeadamente nos equipamentos de apoio, foram utilizadas as ferramentas Angry IP Scanner e Wireshark. Para a análise das Mibs dos equipamentos além da utilização do protocolo SNMP foi também utilizada a ferramenta MIB Browser da iREASONING. O Notepad++ foi uma ferramenta bastante funcional, pois facilitava a visualização e modificação dos ficheiros xml utilizados na importação das configurações de todos os elementos do sistema.

Toda a fase de testes foi realizada com o apoio de equipamento defeituoso, ou com equipamento em funcionamento onde foram postas em prática medidas e configurações, altamente não recomendadas pelos fabricantes dos equipamentos, que permitiram a ocorrência de erros e problemas.

4 Descrição técnica

4.1 Análise e experiências

De modo a ser possível uma tomada uma decisão de quais os pontos que serão marcados como relevantes de serem monitorizados foi necessário realizar inicialmente um estudo de todos os itens que cada equipamento possui. Esse estudo passou pela criação de um ambiente de testes, composto por um *access point* da marca Cisco modelo *Air 1210*, uma *UPS* da marca *Riello* modelo *Netman11* e um *switch* da marca *Nortel* modelo *Nortel 47-24T*. A escolha destes equipamentos foi tomada tendo em conta os seguintes pontos:

- *Switch*, apesar de existirem alguns modelos e marcas de equipamentos, este é o que se encontram em maior numero variando apenas no número de portas que disponibilizavam, todos os outros foram deixados para estudo futuro depois da criação do plano inicial de monitorização.
- *Access Point* e *UPS*, por serem os modelos únicos utilizados por toda a instituição;

De referir que esse estudo foi tendo como base todos os ativos que já estavam a ser monitorizados pelo software *Observium*, mas devido a sua falta de possibilidade de configuração e disposição da informação, foi usado como uma referência de possíveis pontos de monitorização, que foram tomados em conta no estudo efetuado, sendo que este sistema apenas estava configurado para monitorizar os switches, todos os outros elementos tiveram que ser analisados do início.

Este estudo foi dividido em três elementos que foram analisados individualmente sendo criado documentação de modo a poder fomentar mais tarde todas as decisões tomadas.

4.1.1 Switch

No estudo realizado no switch de testes foi efetuada a recolha de todos os elementos disponíveis através do protocolo SNMPv2 que devolveu os respetivos OIDs presentes na MIB, que foram utilizados na elaboração do ficheiro de apoio a replicação e atualização do sistema antigo para o novo, Tabela 4 - Excerto de dados recolhidos da MIB do Switch.

Neste ficheiro estão registadas as análises efetuadas assim como todos os elementos que foram configurados para monitorização, encontrando-se o documento completo em Anexo I – Dados recolhidos da MIB do Switch.

Tabela 4 - Excerto de dados recolhidos da MIB do Switch

Tipo	Nome	OID	Tipo dados	Exemplo
DISMAN-EVENT	DISMAN-EVENT-MIB::sysUpTimeInstance	.1.3.6.1.2.1.1.3.0	Timeticks	2:38:28.43
SNMPv2	SNMPv2-MIB::sysDescr.0	.1.3.6.1.2.1.1.1.0	STRING	Ethernet Switch 470-24T HW:35 FW:3.6.0.7 SW:v3.7.1.08 BN:00 ISVN:2 (c) Nortel Networks
	SNMPv2-MIB::sysName.0	.1.3.6.1.2.1.1.5.0	STRING	Switch Test IPO
	SNMPv2-MIB::sysLocation.0	.1.3.6.1.2.1.1.6.0	STRING	DataCenter Edificio A Piso 2
Interface	IF-MIB::ifOperStatus.1	.1.3.6.1.2.1.2.2.1.8.1	INTEGER	down(2)
	IF-MIB::ifInErrors.1	.1.3.6.1.2.1.2.2.1.14.1	Counter32	0
	IF-MIB::ifOutErrors.1	.1.3.6.1.2.1.2.2.1.20.1	Counter32	0
	IF-MIB::ifInOctets.1	.1.3.6.1.2.1.2.2.1.10.1	Counter32	0
	IF-MIB::ifOutOctets.1	.1.3.6.1.2.1.2.2.1.16.1	Counter32	0
IP	IP-MIB::icmpInErrors.0	.1.3.6.1.2.1.5.2.0	Counter32	0
	IP-MIB::icmpOutErrors.0	.1.3.6.1.2.1.5.15.0	Counter32	0
	IP-MIB::icmpInMsgs.0	.1.3.6.1.2.1.5.1.0	Counter32	29
	IP-MIB::icmpOutMsgs.0	.1.3.6.1.2.1.5.14.0	Counter32	29
	IP-MIB::ipInDelivers.0	.1.3.6.1.2.1.4.9.0	Counter32	25102
TCP	TCP-MIB::tcpActiveOpens.0	.1.3.6.1.2.1.6.5.0	Counter32	0
	TCP-MIB::tcpPassiveOpens.0	.1.3.6.1.2.1.6.6.0	Counter32	0
	TCP-MIB::tcpAttemptFails.0	.1.3.6.1.2.1.6.7.0	Counter32	0
UDP	UDP-MIB::udpInErrors.0	.1.3.6.1.2.1.7.3.0	Counter32	0
	UDP-MIB::udpOutDatagrams.0	.1.3.6.1.2.1.7.4.0	Counter32	27488
EtherLike	EtherLike-MIB::dot3StatsFCSErrors.1	.1.3.6.1.2.1.10.7.2.1.3.1	Counter32	0
	EtherLike-MIB::dot3StatsExcessiveCollisions.1	.1.3.6.1.2.1.10.7.2.1.9.1	Counter32	0
	dot3StatsInternalMacTransmitErrors	.1.3.6.1.2.1.10.7.2.1.10.1	Counter32	0
	dot3StatsCarrierSenseErrors	.1.3.6.1.2.1.10.7.2.1.11.1	Counter32	0
SNMP	SNMPv2-MIB::snmpInPkts	.1.3.6.1.2.1.11.1.0	Counter32	25561
	SNMPv2-MIB::snmpOutPkts	.1.3.6.1.2.1.11.2.0	Counter32	25561

Os elementos de alarmística, como sendo uma parte não implementada no sistema existente, requereu de um estudo mas incisivo sobre quais os elementos importantes de serem marcados assim como quais as condições de serem ativados e desativados novamente, informando o operador dessas mudanças de estado. Erros de comunicação, quer físicos quer lógicos, mudanças de estado de portas (violações) e no próprio estado de funcionamento do aparelho em questão, foram os elementos foram mais focados.

4.1.2 Access Point

No estudo dos access points, foram também efetuadas as mesmas análises da MIB para assim se ficar a saber quais os elementos relevantes de ser monitorizados, Tabela 5 - Excerto de dados recolhidos da Mib do Access Point, encontrando-se em Anexo II - Dados recolhidos da MIB do Access Point.

Tabela 5 - Excerto de dados recolhidos da Mib do Access Point

Tipo	Nome	OID	Tipo dados	Exemplo
System	sysUpTime	1.3.6.1.2.1.1.3	Timeticks	(932774) 2:35:27.74
Interface	ifPhysAddress	1.3.6.1.2.1.2.2.1.6	STRING	0:11:21:cc:86:30
	ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER	down(2)
	ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER	down(2)
	ifLastChange	1.3.6.1.2.1.2.2.1.9	Timeticks	(855) 0:00:08.55
	ifInOctets	1.3.6.1.2.1.2.2.1.10	Counter32	755421
	ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	Counter32	4896
	ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	Counter32	3728
	ifOutDiscards	1.3.6.1.2.1.2.2.1.19	Counter32	0
IP	ifOutErrors	1.3.6.1.2.1.2.2.1.20	Counter32	0
	ipForwarding	1.3.6.1.2.1.4.1	INTEGER	notForwarding(2)
	ipInDiscards	1.3.6.1.2.1.4.8	Counter32	0
	ipInDelivers	1.3.6.1.2.1.4.9	Counter32	6333
	ipOutDiscards	1.3.6.1.2.1.4.11	Counter32	2
	ipOutNoRoutes	1.3.6.1.2.1.4.12	Counter32	0
ICMP	ipRoutingDiscards	1.3.6.1.2.1.4.23	Counter32	0
	icmpInMsgs	1.3.6.1.2.1.5.1	Counter32	2338
	icmpInErrors	1.3.6.1.2.1.5.2	Counter32	0
	icmpInDestUnreachs	1.3.6.1.2.1.5.3	Counter32	4
	icmpInEchos	1.3.6.1.2.1.5.8	Counter32	2334
	icmpOutMsgs	1.3.6.1.2.1.5.14	Counter32	2336
	icmpOutErrors	1.3.6.1.2.1.5.15	Counter32	0
TCP	icmpOutDestUnreachs	1.3.6.1.2.1.5.16	Counter32	4
	icmpOutEchos	1.3.6.1.2.1.5.21	Counter32	0
	tcpActiveOpens	1.3.6.1.2.1.6.5	Counter32	0
	tcpPassiveOpens	1.3.6.1.2.1.6.6	Counter32	234
UDP	tcpInSegs	1.3.6.1.2.1.6.10	Counter32	1684
	tcpOutSegs	1.3.6.1.2.1.6.11	Counter32	2060
	udpInDatagrams	1.3.6.1.2.1.7.1	Counter32	847
SNMP	udpNoPorts	1.3.6.1.2.1.7.2	Counter32	1534
	snmpInPkts	1.3.6.1.2.1.11.1	Counter32	887
	snmpOutPkts	1.3.6.1.2.1.11.2	Counter32	869
	snmpInBadCommunityNames	1.3.6.1.2.1.11.4	Counter32	18
	snmpInBadCommunityUses	1.3.6.1.2.1.11.5	Counter32	0

Foi também efetuado o levantamento das questões importantes sobre quais os pontos críticos a introduzir no sistema de alarmística.

4.1.3 Uninterruptible power supply

A MIB da ups de teste forneceu todos os elementos que foram discriminados e devidamente estudadas, retirando apenas os relevantes para a monitorização permitindo assim ter um conhecimento do seu funcionamento sem perda de recursos com elementos sem interesse,

Tabela 6 – Excerto de dados recolhidos da Mib da UPS.

Tabela 6 – Excerto de dados recolhidos da Mib da UPS

Tipo	Nome	OID	Tipo dados	Exemplo
System	sysUpTimeInstance	.1.3.6.1.2.1.1.3.0	INTEGER	156831
	sysAttachedDevices	.1.3.6.1.2.1.33.1.1.6.0	Hex-STRING	00 00 00 00 00 00 00 00 00 00
Battery	batteryStatus	.1.3.6.1.2.1.33.1.2.1.0	INTEGER	2
	batterySecondsOn	.1.3.6.1.2.1.33.1.2.2.0	INTEGER	0
	batteryEstimatedMinutesRemaining	.1.3.6.1.2.1.33.1.2.3.0	INTEGER	0
	batteryVoltage	.1.3.6.1.2.1.33.1.2.5.0	INTEGER	274
	batteryCurrent	.1.3.6.1.2.1.33.1.2.6.0	INTEGER	0
	batteryTemperature	.1.3.6.1.2.1.33.1.2.7.0	INTEGER	0
Input	inputVoltage	.1.3.6.1.2.1.33.1.3.1.3.1	INTEGER	225
	inputCurrent	.1.3.6.1.2.1.33.1.3.3.1.4.1	INTEGER	0
Output	outputVoltage	.1.3.6.1.2.1.33.1.4.4.1.2.1	INTEGER	223
	outputCurrent	.1.3.6.1.2.1.33.1.4.4.1.3.1	INTEGER	0
Well Known Alarms	upsWellKnownAlarms	1.3.6.1.2.1.33.1.6.3.1		
	upsAlarmChargerFailed	1.3.6.1.2.1.33.1.6.3.13		
	upsAlarmUpsOutputOff	1.3.6.1.2.1.33.1.6.3.14		
	upsAlarmUpsSystemOff	1.3.6.1.2.1.33.1.6.3.15		
	upsAlarmFanFailure	1.3.6.1.2.1.33.1.6.3.16		
	upsAlarmChargerFailed	1.3.6.1.2.1.33.1.6.3.13		
	upsAlarmUpsOutputOff	1.3.6.1.2.1.33.1.6.3.14		
	upsAlarmUpsSystemOff	1.3.6.1.2.1.33.1.6.3.15		
upsAlarmFanFailure	1.3.6.1.2.1.33.1.6.3.16			

A alarmística pensada para este *hardware* foi retirada dos elementos acima em conjunto com os pedidos, e baseiam-se em elementos de excesso de voltagem, potencia e corrente, e falta de carga ou demasiado tempo em carga. Encontrando-se em Anexo III - Dados recolhidos da MIB da UPS todos os dados para consulta.

4.2 Desenvolvimento da solução e testes

O desenvolvimento da solução foi avançando seguindo o plano inicialmente traçado e contemplado no mapa de Gant da fase de desenvolvimento (fase 1). Todas as tarefas foram iniciadas por uma reunião com o coordenador do projeto, definido um objetivo, seguidos de um estudo e configuração, finalizando com um teste. Estas configurações e testes foram realizados de uma forma cíclica de tentativa e erro.

Definição de requisitos

Na fase de definição de requisitos foram estabelecidos todos os moldes que estavam na base da realização do projeto. Foi atingida através de uma reunião como os gestores de projeto, Eng. Renato Magalhães, Diretor do serviço de Informático do IPO Porto, Pedro Alvarenga, elemento da equipa responsável pela rede da instituição e Eng. Hugo Soares, elemento da equipa responsável pelos serviços de monitorização já existentes. Nela foram apresentados os moldes

e objetivos principais e secundários que já estavam em mente antes do início do projeto assim como a inclusão de novos discutidos no decorrer da reunião e que foram estabelecidos como o ponto de partida, assim como algumas ideias iniciais de trabalho futuro como a possibilidade de expansão do projeto a outras áreas de conhecimento. No final foi elaborado o mapa de Gant, Anexo IV - Mapas de Gant, onde se encontra todo o planeamento, dividido em tarefas e os respectivos prazos de conclusão.

Estudo de versões

Antes de se iniciar com a implementação de um ambiente de teste foi necessário fazer um levantamento das várias versões existente da aplicação *Zabbix* e quais as suas diferenças entre elas. Esta tarefa apesar de ser iniciada foi passada a frente, pois como já existia um sistema implementado *Zabbix*, o receio de versões mais recentes não serem compatíveis com o trabalho já elaborado, foi então tomada a decisão de utilizar a versão já instalada (*Zabbix 2.0.3*) em vez da última disponível (*Zabbix 2.2.1*). Em relação ao sistema operativo a ser utilizado este recaiu sobre a última versão do sistema operativo que o serviço de informática institucionalizou como sendo *standard*, Cent OS 6.5.

Instalação de sistema de testes

O objetivo desta tarefa era a criação de um sistema estande de desenvolvimento, composto por um elemento de cada tipo (ativo) na rede a monitorizar, um Switch Nortel 47-24T, um Access Point Cisco Air 1210 e uma UPS Riello Netman11. Para a instalação da aplicação foi criada uma máquina virtual com o sistema operativo Cent OS 6.5, com a versão do *Zabbix 2.0.3*, que ficou definido no estudo da tarefa anterior. Neste ambiente seriam efetuadas todas as recolhas, configurações e teste que tinham que ser realizados para elaborar o estudo de capacidades, sem que estes interfiram com o sistema em produção, que mais tarde servirão para a tomada de decisão dos pontos relevantes para o novo sistema.

Replicação de sistema (Switch)

Depois de devidamente instalado o ambiente de testes, foi necessário também ter acesso ao sistema já implementado em Observium de modo a poder ter um ponto de partida e base de comparação com o que já existe e o que pode vir a ser implementado na passagem para o novo sistema *Zabbix*. Foi então tomada a decisão de fazer uma cópia integral da máquina com o Observium para o ambiente de testes de modo a facilitar esse acesso, sem interferência com o ambiente produtivo. Foi realizado o levantamento/comparativo de todos os itens que o

Observium monitorizava com os que o Switch dispunha, dando origem ao documento final, Anexo V – Estudo integral do Switch. Documento esse que foi depois usado na tomada de decisão de todos os itens que deviam transpor para o novo sistema assim como os que não estavam presentes e que foram marcados como necessários. Foi também decidido que tipo de informação a guardar e através de que método de visualização seria apresentado, Tabela 7 - Excerto do estudo do Switch.

Tabela 7 - Excerto do estudo do Switch

Graficos	Nome	Chave	SNMP OID	Tipo de informação	Intervalo de Recolha (sec)	Valor
SYSTEM	SYSTEM Uptime	sys.UptimeInstance	.1.3.6.1.2.1.1.3.0	Numerico(Decimal)	1 Minuto (60)	As is
	SYSTEM Description	sys.Descr	.1.3.6.1.2.1.1.1.0	Texto	24 Horas (86400)	History (Chassis)
ICMP Informational Statistics	ICMP InRedirects	icmp.InRedirects	.1.3.6.1.2.1.5.7.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	ICMP OutRedirects	icmp.OutRedirects	.1.3.6.1.2.1.5.20.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
IP Statistics	IP InDelivers	ip.InDelivers	.1.3.6.1.2.1.4.9.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	IP InReceives	ip.InReceives	.1.3.6.1.2.1.4.3.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	IP OutDiscards	ip.OutDiscards	.1.3.6.1.2.1.4.11.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	IP OutNoRoutes	ip.OutNoRoutes	.1.3.6.1.2.1.4.12.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
TCP Statistics	TCP InSegs	tcp.InSegs	.1.3.6.1.2.1.6.10.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	TCP OutSegs	tcp.OutSegs	.1.3.6.1.2.1.6.11.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	TCP AttemptFails	tcp.AttemptFails	.1.3.6.1.2.1.6.7.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	TCP EstabResets	tcp.EstabResets	.1.3.6.1.2.1.6.8.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
UDP Statistics	UDP InErrors	udp.InErrors	.1.3.6.1.2.1.7.3.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)
	UDP NoPorts	udp.NoPorts	.1.3.6.1.2.1.7.2.0	Numerico(float)	1 Minuto (60)	Delta (speed per second)

A configuração dos elementos acima recolhidos foi efetuada no novo sistema sendo este dividido em quatro áreas:

- Switch – Dados relativos ao funcionamento geral do switch, informação do equipamento e estatísticas, Anexo V – Estudo integral do Switch;
- Interfaces – Dados recolhidos por interface do Switch, informação da interface e tráfego, Anexo V – Estudo integral do Switch;
- Estatísticas de erros – dados estatísticos dos vários erros de transição de pacotes, Anexo V – Estudo integral do Switch;
- Estatísticas de interface – Dados estatísticos por interface, Anexo V – Estudo integral do Switch;

Estudo de elementos de alarmística (Switch)

Como o sistema Observium não disponibilizava qualquer tipo de definição na criação de uma alarmística, foi necessário analisar os elementos recolhidos e decidir quais os itens que deviam estar integrados nesse novo sistema, assim como decidir os tempos e numero de dados que tenham que acontecer para que seja disparado um problemas e sua respetiva notificação e/ou ação, Tabela 8 - Excerto do estudo de alarmística a definir no switch.

Tabela 8 - Excerto do estudo de alarmística a definir no switch

Nome do Trigger	Condição	Nível
Switch Down	Immediately (0)	Warning
Switch Down (3 Minutes)	3 Minutes (180)	High
Switch Down (1 Hour)	1 Hour (3600)	Disaster
ICMP In Errors	+10 erros for 5 minutes (300)	Warning
ICMP Out Errors	+10 erros for 5 minutes (300)	Warning
UDP In Errors	+10 erros for 5 minutes (300)	Warning
UDP No Ports	+10 erros for 5 minutes (300)	Warning
IF InErrors.1	+10 erros for 5 minutes (300)	Warning
IF OutErrors.1	+10 erros for 5 minutes (300)	Warning
IF InDiscards.1	+10 erros for 5 minutes (300)	Warning
IF OutDiscards.1	+10 erros for 5 minutes (300)	Warning
IF AdminStatus.1	Immediately (0)	Average
IF OperStatus.1	5 Minutes (300)	Warning

Aplicação de alarmística no sistema de testes (Switch)

A aplicação dos elementos alarmísticos, não se baseou apenas em configurá-los no sistema, foi necessário definir configurações condicionais para que, questões como falsos positivos por picos de valores, não sejam despoletados. Assim a implementação de condições/regras como só ser considerado como um problema real se, por exemplo, o registo de ocorrência de erros se mantiver constante durante um determinado período de tempo. Outra funcionalidade que foi implementada foi a escalabilidade de problemas, ou seja à medida que o problema se mantém ao longo do tempo, este vai escalando quanto a sua gravidade, sendo tomadas outras ações ou formas de notificar os elementos chave da equipa, Anexo VI – Estudo completo da alarmística do Switch.

Testes do sistema

Estes testes apenas decorreram no ambiente de testes e tiveram como finalidade testar a configuração dos itens, se estavam corretos e a devolver os dados devidos. Também foram testados os intervalos de tempo de recolha se se adequavam ao item referente e se os gráficos criados com a informação apresentavam a informação correta, visível e de fácil entendimento.

Estes testes basearam-se em efetuar ligação ao Switch de equipamento sem problemas assim como equipamento defeituoso para que haja uma recolha de dados diversificados, abrangendo o máximo de itens possíveis, permitindo assim também testar a alarmística.

Replicação de sistema (UPS)

Os bastidores principais da infraestrutura de rede da instituição são suportados por uma fonte de energia ininterrupta (Uninterruptible Power Supply), que em caso de falta de energia, ou flutuação de potência, evitam que o bastidos ser desligue abruptamente ou tenha danos elétricos. Por essa razão, a monitorização desse equipamento se torna importante, para garantir que problemas de maior relevância não aconteçam, Tabela 9 - Excerto do estudo da UPS.

Este tipo de equipamento também não se encontrava abrangido no sistema Observium, sendo necessário um estudo mais aprofundado quanto a funcionalidade e potencial dos itens existentes nas UPS. No documento em Anexo VII - Estudo integral da UPS, pode-se ver na íntegra todos os itens analisados e que foram passados para o sistema.

Tabela 9 - Excerto do estudo da UPS

Gráficos	Nome	Chave	SNMP OID	Tipo de informação	Intervalo de Recolha (sec)	Valor
SYSTEM	SYSTEM Uptime	sys.UpTime	.1.3.6.1.2.1.1.3.0	Numeric(Decimal)	1 Minute (60)	As is
	SYSTEM Attached Devices	sys.AttachedDevices	.1.3.6.1.2.1.33.1.1.6.0	Text	24 Hours (86400)	History (Notes)
Battery	BATTERY Status	battery.Status	.1.3.6.1.2.1.33.1.2.1.0	Charecter	5 Minutes (300)	APC Battery Status
	BATTERY Seconds On Battery	battery.SecondsOnBattery	.1.3.6.1.2.1.33.1.2.2.0	Numeric(Decimal)	2 Minutes (120)	As Is
	BATTERY Estimated Minutes Remaining	battery.EstimatedMinutesRemaining	.1.3.6.1.2.1.33.1.2.3.0	Numeric(Decimal)	2 Minutes (120)	As Is
	BATTERY Voltage	battery.Voltage	.1.3.6.1.2.1.33.1.2.5.0	Numeric(Float)	1 Minute (60)	As Is
	BATTERY Current	battery.Current	.1.3.6.1.2.1.33.1.2.6.0	Numeric(Decimal)	1 Minute (60)	As Is
Input	BATTERY Temperature	battery.Temperature	.1.3.6.1.2.1.33.1.2.7.0	Numeric(Float)	1 Minute (60)	As Is
	INPUT Voltage	input.Voltage	.1.3.6.1.2.1.33.1.3.3.1.3.1	Numeric(Float)	1 Minute (60)	As Is
Output	INPUT Current	input.Current	.1.3.6.1.2.1.33.1.3.3.1.4.1	Numeric(Float)	1 Minute (60)	As Is
	OUTPUT Voltage	output.Voltage	.1.3.6.1.2.1.33.1.4.4.1.2.1	Numeric(Float)	1 Minute (60)	As Is
Bypass	OUTPUT Current	output.Current	.1.3.6.1.2.1.33.1.4.4.1.3.1	Numeric(Float)	1 Minute (60)	As is
	BYPASS Voltage	bypass.Voltage	.1.3.6.1.2.1.33.1.5.3.1.2.1	Numeric(Float)	1 Minute (60)	As is
	BYPASS Current	bypass.Current	.1.3.6.1.2.1.33.1.5.3.1.3.1	Numeric(Float)	1 Minute (60)	As is
	BYPASS Power	bypass.Power	.1.3.6.1.2.1.33.1.5.3.1.4.1	Numeric(Float)	1 Minute (60)	As is

Estudo de elementos de alarmística (UPS)

Os passos desta tarefa foram os mesmos que os efetuados no estudo do Switch, Tabela 10 - Excerto do estudo de alarmística a definir nas UPS, mas foram focadas questões mais técnicas como valores de entrada e saída de corrente e potencia, se estava a passar carga para o bastidor ou se era de fonte externa, tempos de utilização e eminente descarga total.

Tabela 10 - Excerto do estudo de alarmística a definir nas UPS

Nome do trigger	Condição	Severity
Battery Low	Immediately (0)	Warning
Battery Depleted	Immediately (0)	High
Device On Battery	Immediately (0)	Information
Device On Battery (5 Minutes)	On for 5 minutes (300)	Warning
Device On Battery (10 Minutes)	On for 10 minutes (600)	High
15 Minutes Of Battery Left	Immediately (0)	Warning
10 Minutes of Battery Left	Immediately (0)	Average
5 Minutes of Battery Left	Immediately (0)	High
1 Minute of Battery Left	Immediately (0)	Disaster
Battery Not Fully Charged	Immediately (0)	Information
Battery Voltage Too High	bVol > 230 for 2 minutes (120)	Warning
Battery Current Too High	bCurr > 4 for 2 minutes (120)	Warning
Battery Temperature Too High	Temp > 60º for 5 minutes (300)	Warning
Battery Temperature Too High (15 Minutes)	Temp > 60º for 15 minutes (900)	High
Input Too Many Line Bads	iLnbad > 5	Warning
Input Frequency Too High	iFreq > 600 for 2 minutes (120)	Warning
Input Voltage Too High	iVol > 275 for 2 minutes (120)	Warning
Input Current Too High	iCurr > 4 for 2 minutes (120)	Warning
Output Frequency Too High	oFreq > 600 for 2 minutes (120)	Warning
Output Voltage Too High	oVol > 235 for 2 minutes (120)	Warning
Output Current Too High	oCurr > 4 for 2 minutes (120)	Warning
Output Power Too High	oPwr > 500 for 2 minutes (120)	Warning
Output Percent Load Too High	oPerLd > 90 for 2 minutes (120)	Warning
Bypass Frequency Too High	bFreq > 600 for 2 minutes (120)	Warning
Bypass Voltage Too High	bVol > 230 for 2 minutes (120)	Warning
Bypass Current Too High	bCurr > 4 for 2 minutes (120)	Warning
Bypass Power Too High	bPwr > 500 for 2 minutes (120)	Warning

Aplicação de alarmística no sistema de testes (UPS)

Neste passo, em específico, a definição das condições foi auxiliada por elemento da equipa do SIET, nas questões relacionadas com intervalos de valores aceitáveis no que diz respeito a frequência, potência, voltagem, etc, para a definição dos alarmes, Anexo VIII - Estudo completo da alarmística da UPS.

Testes do sistema

O plano de testes manteve-se para este equipamento, foi ligado ao ambiente de teste uma ups com problemas nas baterias, foram avaliados a receção dos valores de entrada e de saída e ao

efetuar o desligamento dos equipamentos da corrente os alarmes e tempos de carga foram também testados.

Replicação de sistema (AP)

Como no caso das UPS, também os Access Point não estavam inseridos no Observium. Apesar de o número de equipamentos ser reduzido, limitado apenas ao edifício principal (edifício A), piso 3, andar onde estão localizadas as clínicas do IPO Porto, que fornecem um serviço de internet gratuito aos utentes da instituição.

Com este equipamento foi necessário efetuar o estudo de dados, Anexo IX - Estudo integral do Access Point, referente a conectividade entre o servidor e o Access Point, assim como da dispersão do sinal, Tabela 11 - Excerto do estudo do Access Point.

Tabela 11 - Excerto do estudo do Access Point

Graficos	Nome	Chave	SNMP OID	Tipo de informação	Intervalo de Recolha (sec)	Valor
System	SYSTEM Uptime	sys.UpTime	.1.3.6.1.2.1.1.3.0	Numeric(Decimal)	1 Minute (60)	As is
Interface	IF PhysAddress.Ra0	if.PhysAddress.Ra0	.1.3.6.1.2.1.2.2.1.6.1	Text	24 Hours (86400)	
	IF AdminStatus.Ra0	if.AdminStatus.Ra0	.1.3.6.1.2.1.2.2.1.7.1	Charecter	1 Hour (3600)/1 Minute (60)	SNMP interface status (ifAdminStatus)
	IF OperStatus.Ra0	if.OperStatus.Ra0	.1.3.6.1.2.1.2.2.1.8.1	Charecter	1 Hour (3600)/1 Minute (60)	SNMP interface status (ifOperStatus)
	IF LastChange.Ra0	if.LastChange.Ra0	.1.3.6.1.2.1.2.2.1.9.1	Numeric(Decimal)	1 Hour (3600)	As is
Traffic	IF InOctets.Ra0	if.InOctets.Ra0	.1.3.6.1.2.1.2.2.1.10.1	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	IF InUcastPkts.Ra0	if.InUcastPkts.Ra0	.1.3.6.1.2.1.2.2.1.11.1	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	IF InMulticastPkts.Ra0	if.InMulticastPkts.Ra0	.1.3.6.1.2.1.2.2.1.12.1	Numeric(Float)	1 Minute (60)	Delta (speed per second)
Errors	IF OutDiscards.Ra0	if.OutDiscards.Ra0	.1.3.6.1.2.1.2.2.1.19.1	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	IF OutErrors.Ra0	if.OutErrors.Ra0	.1.3.6.1.2.1.2.2.1.20.1	Numeric(Float)	1 Minute (60)	Delta (speed per second)
IP Statistics	IP Forwarding	ip.Forwarding	.1.3.6.1.2.1.4.1.0	Charecter	1 Hour (3600)	Forwarding State
	IP InDiscards	ip.InDiscards	.1.3.6.1.2.1.4.8.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	IP InDelivers	ip.InDelivers	.1.3.6.1.2.1.4.9.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	IP OutDiscards	ip.OutDiscards	.1.3.6.1.2.1.4.11.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	IP OutNoRoutes	ip.OutNoRoutes	.1.3.6.1.2.1.4.12.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	IP ForwDatagrams	ip.ForwDatagrams	.1.3.6.1.2.1.4.6.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
IP Errors	IP RoutingDiscards	ip.RoutingDiscards	.1.3.6.1.2.1.4.23.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
ICMP Statistics	ICMP InMsgs	icmp.InMsgs	.1.3.6.1.2.1.5.1.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	ICMP InErrors	icmp.InErrors	.1.3.6.1.2.1.5.2.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	ICMP InDestUnreachs	icmp.InDestUnreachs	.1.3.6.1.2.1.5.3.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	ICMP InEchos	icmp.InEchos	.1.3.6.1.2.1.5.8.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	ICMP OutMsgs	icmp.OutMsgs	.1.3.6.1.2.1.5.14.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	ICMP OutErrors	icmp.OutErrors	.1.3.6.1.2.1.5.15.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	ICMP OutDestUnreachs	icmp.OutDestUnreachs	.1.3.6.1.2.1.5.16.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	ICMP OutEchos	icmp.OutEchos	.1.3.6.1.2.1.5.21.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
TCP Statistics	TCP ActiveOpens	tcp.ActiveOpens	.1.3.6.1.2.1.6.5.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	TCP PassiveOpens	tcp.PassiveOpens	.1.3.6.1.2.1.6.6.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	TCP InSegs	tcp.InSegs	.1.3.6.1.2.1.6.10.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	TCP OutSegs	tcp.OutSegs	.1.3.6.1.2.1.6.11.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
UDP Statistics	UDP InDatagrams	udp.InDatagrams	.1.3.6.1.2.1.7.1.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	UDP NoPorts	udp.NoPorts	.1.3.6.1.2.1.7.2.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
SNMP Packet Type Statistics	SNMP InPkts	snmp.InPkts	.1.3.6.1.2.1.11.1.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	SNMP OutPkts	snmp.OutPkts	.1.3.6.1.2.1.11.2.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
SNMP Errors	SNMP InBadCommunityNames	snmp.InBadCommunityNames	.1.3.6.1.2.1.11.4.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)
	SNMP InBadCommunityUses	snmp.InBadCommunityUses	.1.3.6.1.2.1.11.5.0	Numeric(Float)	1 Minute (60)	Delta (speed per second)

Estudo de elementos de alarmística (AP)

Toda a alarmística deste equipamento baseou-se em excesso de erros por parte da conectividade, quer com o servidor, quer como a transmissão de dados pelo meio. O estado do seu funcionamento também foi adicionado na alarmística, Tabela 12 - Excerto do estudo de alarmística a definir no Access Point.

Tabela 12 - Excerto do estudo de alarmística a definir no Access Point

Nome do trigger	Condição	Nível
Access Point Down	Immediately (0)	Warning
Access Point Down (3 Minutes)	3 Minutes (180)	High
Access Point Down (1 Hour)	1 Hour (3600)	Disaster
ICMP In Errors	+10 erros for 5 minutes (300)	Warning
ICMP Out Errors	+10 erros for 5 minutes (300)	Warning
ICMP In DestUnreachs	+10 erros for 5 minutes (300)	Warning
ICMP Out DestUnreachs	+10 erros for 5 minutes (300)	Warning
IP RoutingDiscards	+10 erros for 5 minutes (300)	Warning
IP In HdrErrors	+10 erros for 5 minutes (300)	Warning
IP In AddrErrors	+10 erros for 5 minutes (300)	Warning

Aplicação de alarmística no sistema de testes (AP)

A configuração da alarmística deste equipamento foi dividida em duas partes, uma relativa apenas às conexões entre o servidor e o Access Point, rede física, e a segunda nos possíveis problemas e informação com a rede sem fios, Anexo X - Estudo completo da alarmística do Access Point.

Testes do sistema

Os testes realizados com este equipamento foram auxiliados por um computador portátil, com uma placa de rede sem fios e foram testados diversos cenários de funcionalidade e falhas, quer a nível de rede física como rede sem fios.

Estudo e aplicação da disposição da informação

Toda esta recolha dos elementos dos vários aplicativos de pouco serve se não for pensada uma forma de disponibilizar a informação de uma forma que, rapidamente e intuitivamente, se possa visualizar e analisar os estados, erros e funcionamento destes mesmos. Assim foram criados vários conjuntos de gráficos, agrupando vários elementos, que permitem uma comparação e descobrir a possível causa de problemas apenas com a sua visualização, tornando a resolução desse problema mais incisiva, indo ao centro do problema, evitando vários passos

de troubleshooting, ganhando tempo e evitando perda de serviço/recursos, pois essa procura pelo problemas no cenário atual tinha que haver primeiro um contacto do utilizador final reportando essa falha.

A Figura 14 - Gráfico de tráfego, apenas é um exemplo de um dos gráficos produzidos pelo sistema, existindo uma variedade de gráficos que passa por estatísticas, quer de estatísticas dos aparelhos, estatísticas de cada porta e também de gráficos ao segundo que mostram em tempo real o que esta a acontecer.

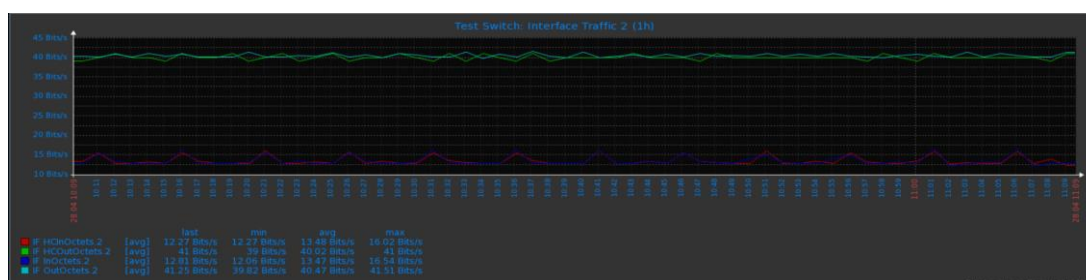


Figura 14 - Gráfico de tráfego

A Tabela 13 – Listagem de gráficos criados apresenta uma tabela com o tipo de gráfico e respetivos nomes assim como qual a informação que o mesmo apresenta.

Tabela 13 – Listagem de gráficos criados

	Graph Type	Graph Name	Information
Switch	Statistics	ICMP Informational Statistics	In/Out ICMP Address Mask/Redirects/Source Quenchs
		ICMP Statistics	In/Out ICMP Echos/Errors/Messages
		IP Fragmentation Statistics	IP Frags/Reasm Status
		IP Statistics	In/Out IP Delivers/Discards/Receives
		SNMP Packet Type Statistics	In/Out SNMP Packets
		SNMP Statistics	In/Out SNMP Pollers
		TCP Statistics	TCP Connectios Status
	UDP Statistics	In/Out UDP Datagrams and errors	
	Interface	Traffic	In/Out Octets
		Unicast Packets	In/Out Unicast Packets
		Non Unicast Packets	In/Out Broadcast/Multicast/Not Unicast Packets
		Errors	In/Out Errors and Discards
		Unknwon Protocols	Unknwon Protocols
	Interface Statistics	EtherLike Stats	Collisions and errors in more deep
		Errors	Errors, collisions and drops
Octets		Quantity of octets	
Packets Size		Average size of packets	
Traffic		Traffic that pass on the interface	
Access Point	Statistics	ICMP Informational Statistics	In/Out ICMP Address Mask/Redirects/Source Quenchs
		ICMP Statistics	In/Out ICMP Echos/Errors/Messages
		ICMP Time Statistics	In/Out Time Exceeds/Stamps
		IP Errors	IP Address/Headers Errors, Unknown Protocols and Route Discards
		IP Fragmentation Statistics	IP Frags/Reasm Status
		IP Statistics	In/Out IP Delivers/Discards/Receives
		SNMP Errors	SNMP Related Errors
		SNMP Packet Type Statistics	In/Out SNMP Packets
		SNMP Statistics	In/Out SNMP Pollers
		TCP Errors	In/Out TCP Errors
		TCP Statistics	TCP Connectios Status
	UDP Statistics	In/Out UDP Datagrams and errors	
	Interface	Errors	In/Out Errors and Discards
		Non Unicast Packets	In/Out Broadcast/Multicast/Not Unicast Packets
		Traffic	In/Out Octets
Unicast Packets		In/Out Unicast Packets	
Unknwon Protocols		Unknwon Protocols	
UPS	Status	Battery	Current, Voltage and Temperature
		Battery Times	Estimated Charge/Minutes and Seconds on Battery
		Bypass	Bypass Current, Voltage, Power and Frequency
		Config	Native Configuration
		Input	Input Current, Voltage, Power and Frequency
		Output	Output Current, Voltage, Power and Frequency

Estes gráficos existem para facilitar a resolução de um evento anormal, permitindo uma ajuda na análise de onde, quando e porque esse evento ocorreu.

Decisão Tecnológica

A tarefa final da primeira fase ficou estabelecida como a análise/fusão de todos os elementos acima referidos e todo o trabalho, quer de configuração, teste e aplicação, ficando decidido todos os pontos que deveriam passar para a segunda fase, a de implementação das configurações em ambiente de testes para o ambiente de produção.

Antes da transição para a fase seguinte foi requisitado uma explicação mais fundamentada de como funcionava o sistema de notificações do Zabbix. Foi então elaborado o documento que se encontra em Anexo XI - Processo de envio de notificações na íntegra, de modo a permitir aos elementos da equipa, findo este estágio, perceber a lógica e sequência de eventos necessários na criação de notificações/ações de modo a que futuras ações possam ser introduzidas no sistema.

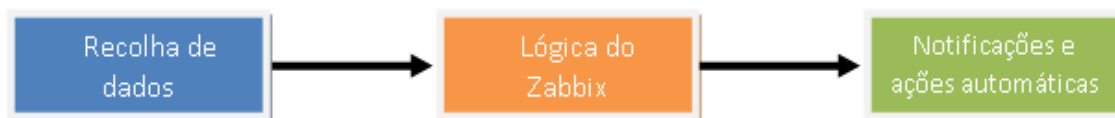


Figura 15 - Logica do zabbix

A passagem da fase de testes para produção, segunda fase do projeto, manteve o mesmo modo de trabalho da primeira fase, existindo a reunião e definição de objetivos, estudo, configuração e testes. No final foram tiradas as devidas conclusões sobre o que foi feito e o que falhou, como foi feito e o que é possível ser feito para o futuro.

Definição de Nomes

De forma a criar um sistema que todos os elementos da equipa do serviço de informática entendam foi necessário reunir com a equipa toda e definir todo um conjunto de nomenclaturas que rapidamente permita identificar qual o equipamento em questão, função e sua localização.

Criação de novos hostgroups

Com a nova informação decidida no ponto anterior criou-se a necessidade de criação de novos grupos que permitissem a separação dos equipamentos por tipo e função, criando assim um sistema mais fácil de entender e perceber a fonte do problema. Foram então criados três novos grupos:

- Rede – Todos os ativos de rede foram introduzidos neste grupo. Switches , Access Points, Concentradores de rede foram depois divididos em subgrupos mais pequenos;
- Apoio – Todo o equipamento de apoio a infraestrutura da instituição (UPS);
- Servidores – Os elementos que já existiam referentes aos servidores da instituição foram transpostos para este grupo.

Importar Templates

A importação dos templates para os 94 equipamentos foi sendo executada de uma forma gradual, para que deste modo, possíveis erros na importação possam ser detetados e corrigidos de imediato, para que não causem problemas nas tarefas adiante. Estes templates foram criados e testados no ambiente de testes mas nesta transição tiveram que ser novamente testados de modo a garantir a total funcionalidade dos mesmos, sendo necessário adapta-los aos equipamentos, pois nem todos os Switches são da mesma marca e modelo do utilizado no ambiente de testes.

Criação de novos hosts

Todos os equipamentos(hosts) que não existiam no sistema tiveram que ser criados e testados para confirmar que comunicavam com o servidor Zabbix e que transmitiam a informação desejada.

Criação de mapas

Criar um mapa por edifício e por andar, foi uma das formas encontradas de visualização de problemas. Foi necessário ter acesso às plantas de cada edifício e respetivo andar para se poder posicionar no devido lugar todo o equipamento existente nesse mesmo andar, facilitando assim aos elementos da equipa, na eventualidade de ser necessário a deslocação ao local para resolução do problema, saber a sua localização exata.

Importar mapas

Finalizando a criação dos mapas de todos os edifícios da instituição, estes foram importados para o novo sistema, permitindo assim ser acedidos por todos os intervenientes do sistema.

Criação de screens

Para uma monitorização mais geral foi criado um dashboard, Figura 16 - Dashboard do sistema, que mostra o estado do sistema como um todo. Este dashboard foi dividido em quatro secções:

1. Estado do servidor de Zabbix - Mostra o estado do servidor de Zabbix, mostrando estatística de todos os hosts, itens e triggers presentes no sistema assim como os seus estados;
2. Triggers Info por grupo - Nesta secção são apresentados os estados de todos os triggers presente no sistema, divididos pelo seu grupo. Esta secção permite, de uma forma

rápida, verificar em que grupo o problema se encontra, reduzindo assim a procura de elementos;

3. Estado do Sistema - O estado do sistema permite, não só perceber onde está o problema, mas também a quantidade de problemas por grupo e a sua gravidade.

Para além da quantidade e gravidade de problemas por grupo, permite de uma forma simples e rápida perceber também qual o problema, em que host e a quanto tempo este problema esta a manifestar-se;

4. Histórico de eventos - O histórico de eventos permite analisar as mudanças dos vários eventos, mostrando quando ocorreram, em que aparelho, qual o problema, o seu estado e a sua gravidade. Com esta informação pode-se analisar possíveis padrões de acontecimentos, se acontecem sempre a mesma hora, se é sempre a mesma maquina a ter problemas, assim como outra informação relevante que fornece um melhor entendimento dos problemas e facilita a sua resolução.

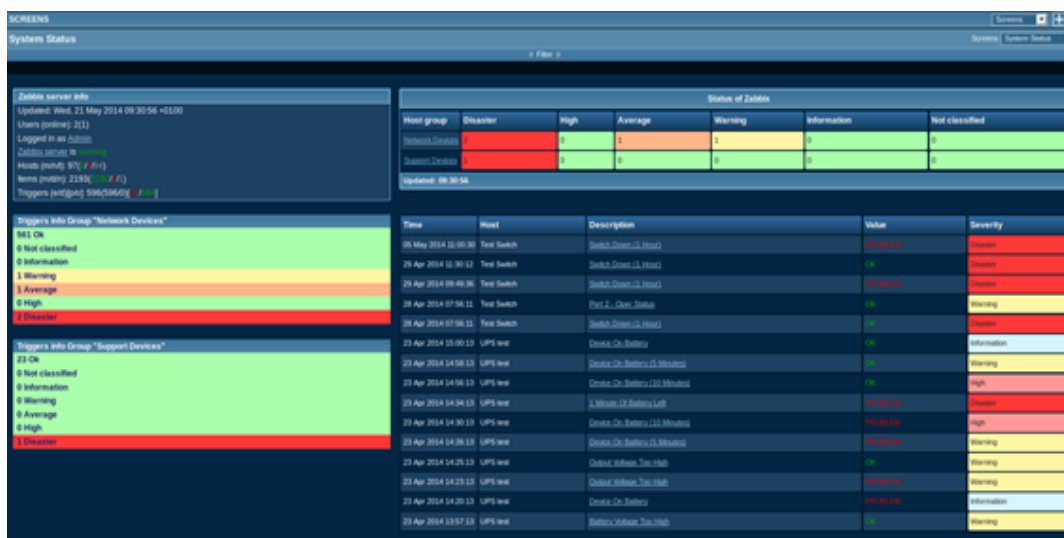


Figura 16 - Dashboard do sistema

Importação de screens

Gráficos, mapas e tabelas foram embebidos nesses ecrãs, foram importados e testados, confirmando que mostravam a informação desejada sem falhas e de forma passível de ser entendida por toda a equipa.

Criação de slide show

A possibilidade de ter um modo de visualização da informação que permita abranger todos os pontos críticos sem constante interação com o sistema foi um dos fatores de escolha do software.

Foi criado, utilizando a funcionalidade de Slide Show do Zabbix, uma ordem sequencial de ecrãs que se revezam de 10 em 10 segundos, sendo o primeiro ecrã o dashboard do sistema, percorrendo a lista que é composta por mapas dos pontos mais relevantes da instituição e gráficos de desempenho.

Testes do sistema

O último passo foi a criação de um conjunto de testes que abrangessem todos os itens de todos os equipamentos, assim como testes de carga para verificar como o sistema se comportaria em casos extremos. Nos testes dos elementos configurados quer de monitorização quer de alarmística, foram detetados alguns problemas que foram sendo corrigidos mediante a sua aparição. Com pouca carga verificou-se que o sistema funcionava sem problemas, recolhendo os dados e detetando os problemas que foram intencionalmente criados.

Com o aumento de carga, o sistema começou a mostrar falhas no tratamento de toda a informação, inicialmente a dar falsos positivos por atraso da leitura dos dados e perda de valores, até ao colapso total do sistema.

Decisão Tecnológica

A análise final do sistema revelou que, a transição de todos os elementos já monitorizados pelo sistema Observium foi concluída com sucesso, assim como a adição dos novos elementos. A criação da alarmística também revelou-se acima da expectativa inicial pois permitia ao serviço de informática um novo modus operandi, pois evitava que a deteção de problemas tivesse que ser reportado através de fonte externa ao serviço, podendo assim fornecer um ação mais incisiva sobre o problema, antes mesmo de este causar transtorno, e permitindo que medidas possam ser tomadas de antemão, atenuando possíveis ambientes de desastre.

Foram também tomadas em conta o planeamento de novas medidas de resolução automátatas de certos problemas que, de outra maneira, necessitavam de intervenção humana na resolução.

Foi também observado que o hardware que compunha o sistema, com estas novas funcionalidades se demonstrou insuficiente para efetuar o tratamento da informação e manter

o sistema estável, percebendo-se da necessidade de planeamento de um novo sistema que consiga suportar o sistema assim como margem de manobra para futura expansão. Foi tomada a decisão de elaborar um estudo de uma nova arquitetura de alta disponibilidade, pensada com medidas de segurança e replicação dos dados, capaz de manter o sistema sempre disponível e fiável.

4.3 Proposta de solução alternativa

Devido ao facto do sistema não conseguir acompanhar com todas as novas configurações surgiu a necessidade de planear e projetar uma nova arquitetura que permitisse não só incluir essas configurações, mas também habilitar o novo sistema de medidas que permitiam uma maior performance, disponibilidade e segurança do sistema e de toda a informação.

O sistema em produção baseava-se numa arquitetura simples que, apesar de funcional, continha muitas lacunas no que diz respeito a disponibilidade e segurança, Figura 17 - Diagrama da arquitetura em produção, pois existia um único componente que, na eventualidade de falha ou corrupção da informação, se revelaria fatal para todo o sistema. A performance do mesmo também sofria significativamente devido a confluência de todos os dados para um único ponto, que em número elevado levava a perda de informação algo que não era aceitável para a instituição.

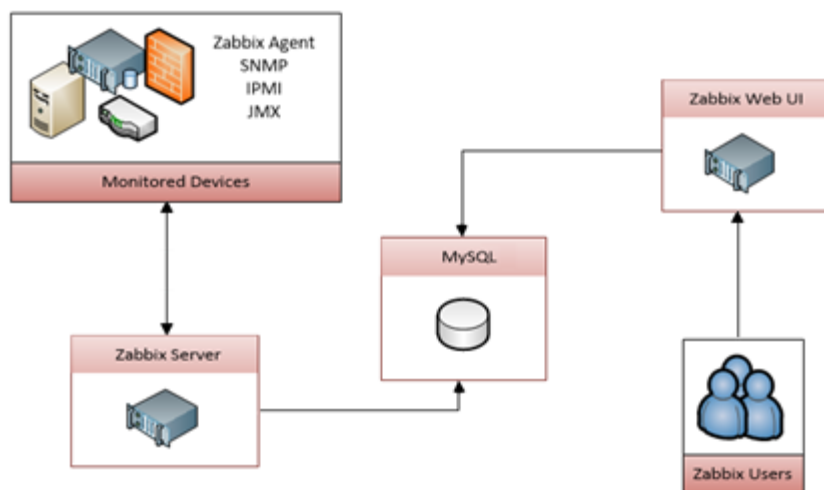


Figura 17 - Diagrama da arquitetura em produção

A inclusão dos novos elementos mostra uma enorme disparidade de valores em comparação com os valores dos elementos já existentes. Na Figura 18 - Valores dos novos elementos é possível

observar o número de novos elementos que terão que estar incluídos no sistema que em comparação com o que existe, Figura 19 – Valores dos elementos existentes, é possível quantificar o salto no incremento de valores.

Host			Items			Triggers		
Host	Type	Hosts	Items	Host/Type	Total/Type	Triggers	Host/Type	Total/Type
Switch	24	4	1814	4	7256	487	4	1948
Switch	24 - 24	1	3504	1	3504	960	1	960
Switch	24 - 50	1	5402	1	5402	1480	1	1480
Switch	48	15	3566	15	53490	967	15	14505
Switch	48-24	1	5256	1	5256	1440	1	1440
Switch	48-48	15	7008	15	105120	1920	15	28800
Switch	48 - 48 - 24	1	8760	1	8760	2400	1	2400
Switch	48 - 48 - 48	1	10512	1	10512	2880	1	2880
Switch	48 - 48 - 48 - 48	1	14016	1	14016	3840	1	3840
Switch	50	2	3712	2	7424	1007	2	2014
Switch	50 - 48	1	7154	1	7154	1960	1	1960
Switch	50 - 50	3	7362	3	22086	2007	3	6021
Partial Totals		46	78066	46	249980	21348	46	68248
Access Point	Cisco	13	186	13	2418	40	13	520
Partial Totals		13	186	13	2418	40	13	520
UPS	Riello	46	47	46	2162	27	46	1242
Partial Totals		46	47	46	2162	27	46	1242
Totals		105	78299	105	254560	21415	105	70010

Figura 18 - Valores dos novos elementos

Status of Zabbix		
Parameter	Value	Details
Zabbix server is running	Yes	127.0.0.1:10051
Number of hosts (monitored/not monitored/templates)	497	124 / 74 / 299
Number of items (monitored/disabled/not supported)	3061	1399 / 1188 / 274
Number of triggers (enabled/disabled) [problem/ok]	933	843 / 90 [17 / 826]
Number of users (online)	20	3
Required server performance, new values per second	20.61	-
Updated: 14:38:53		

Figura 19 – Valores dos elementos existentes

Este estudo teve em consideração este aumento permitindo, ao mesmo tempo, escalar estes valores tendo em conta futuras adições de novos equipamentos e desenvolvimentos que não foram integrados inicialmente no desenho/implementação do novo sistema, por não serem considerados relevantes no presente.

Foi pensada então a nova arquitetura, Figura 20 – Diagrama da nova arquitetura, tendo em mente também a limitação dos recursos disponíveis no serviço de informática, baseando-se numa arquitetura de alta disponibilidade e de alto desempenho (HA).

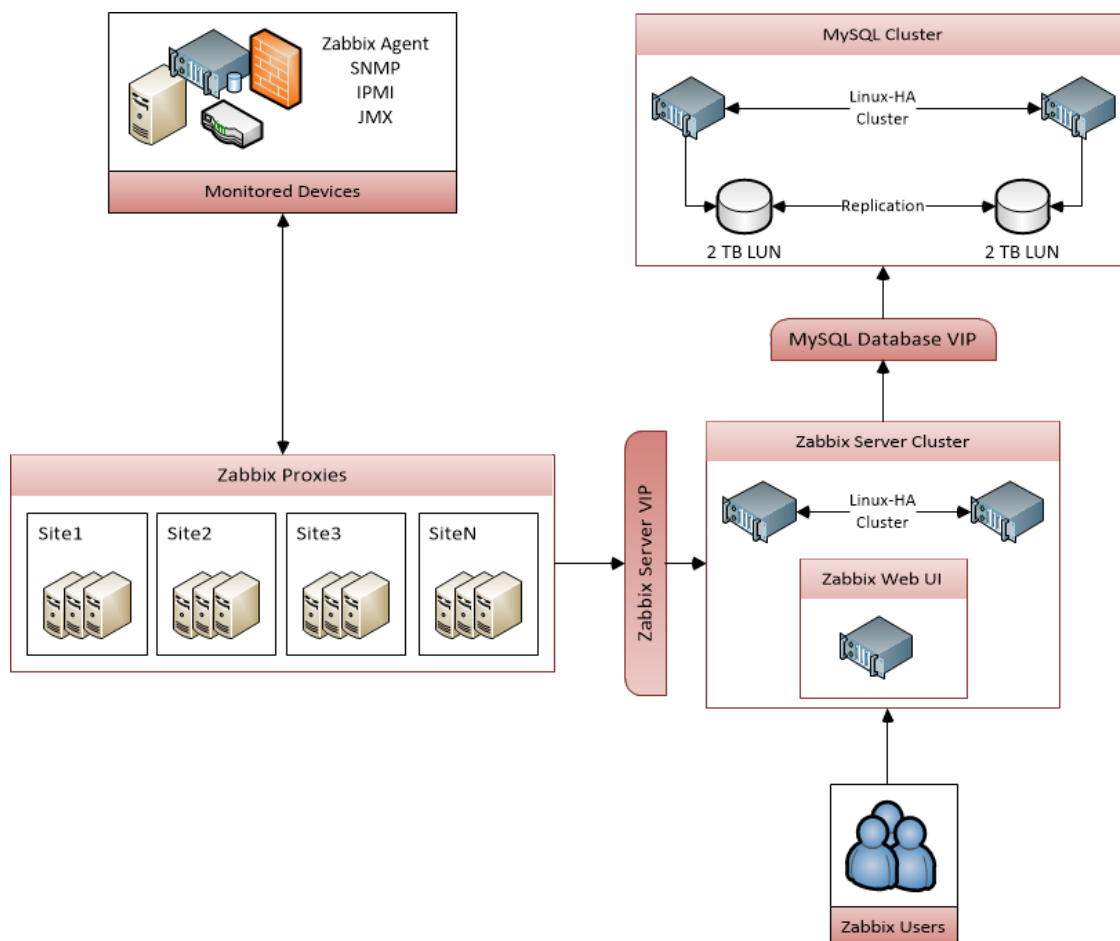


Figura 20 – Diagrama da nova arquitetura

Foi então proposta a criação de dois *clusters* no sistema, um para a base de dados, sendo o outro para o servidor *Zabbix*.

O cluster de base de dados têm que estar capacitado de um poder de leitura e escrita de dados bastante elevado devido à elevada carga de informação por ele tem que passar. Aconselhadamente deve ser configurado como ativo-ativo e ser composto por 2 TB LUN replicáveis entre si, criando assim um ambiente disponível, redundante e seguro.

O cluster do servidor Zabbix configurado como ativo-passivo, deve ter um bom poder de processamento pois é o responsável pelos pedidos e análise da informação recolhida,

despoletando os vários eventos e ações. Neste deve estar embebido a interface Web onde vão ser apresentados todos os ecrãs e mapas criados.

A inclusão de proxies no sistema irá permitir a eliminação de bottleneck no servidor Zabbix pois permite a divisão da recolha, ou seja o processamento de pedidos e recolha caia sobre a proxy e não sobre o servidor, aumentando ao mesmo tempo a segurança pois cada proxy tem em si configurada uma base de dados local que armazena todos os dados antes de os enviar para o servidor, evitando assim a perda de informação.

Estas proxies deverão ser divididas em três grupos separados pela sua função:

- Servidores e bases de dados - Onde estão inseridos todos os servidores e bases de dados de toda a instituição;
- Ativos de rede – Onde está inserido todo o equipamento de rede;
- Equipamentos de suporte – Equipamentos de suporte a instituição serão introduzidos neste grupo.

Na eventualidade de no futuro novos grupos tenham que ser criados, esta arquitetura permite a adição dos mesmos sem necessidade de grandes configurações.

A nível de hardware, e como mencionado acima, foi necessário jogar com os recursos que o IPO Porto possuía, para a apresentação desta proposta, Figura 21 – Proposta de configuração do sistema. Ao nível dos clusters de base de dados e do servidor é importante que estes possam ser máquinas físicas, dedicadas apenas para este fim, devido a necessidade de processamento e leitura/escrita. Quanto as proxies estas podem ser virtualizadas pois não necessitam de grande poder de processamento. Foi também proposto a instalação da última versão dos aplicativos, quer das bases de dados, quer do Zabbix pois permitiam um acréscimo de configuração e desempenho. De referenciar que a ultima versão do Zabbix permitia já a recolha de dados SNMP em Bulk em vez de um de cada vez, o que trás um decremento no numero de pedidos aumentando assim o desempenho de todo o sistema.

Zabbix server	Zabbix database	Zabbix proxies	SAN
12x cores 4GB memory 128GB disk CentOS 6.5 x64 Zabbix 2.2.4	12x cores 8GB memory 2TB SAN CentOS 6.5 x64 MySQL 5.6.12+	4x cores 2GB memory 50GB disk CentOS 6.5 x64 Zabbix 2.2.4 MySQL 5.6.12+	2x 2TB LUN

Figura 21 – Proposta de configuração do sistema

Todo o sistema foi pensado para fornecer um alto desempenho e disponibilidade, tendo para isso ter em conta as configurações dos clusters e proxies.

Sumarizando os vários pontos mais importantes a ter em conta, assim como outras propostas, de modo a se poder obter um sistema estável, fiável, sem perdas de informação ou de serviço e ao mesmo tempo escalável:

- Ter o servidor e a base de dados a executar em sistema separados;
- Particionar sempre que possível as tabelas da base de dados;
- Definir os intervalos de atualização dos vários itens com tempos realistas;
- Utilizar proxies para monitorizar conjuntos de equipamentos equiparáveis;
- Manter um controlo sobre a performance da base de dados (esta ao crescer vais necessitar de afinamento);
- Planear os templates com antecedência de modo a não se ter que andar constantemente a altera-los;
- Limitar o número de utilizadores com acesso ao servidor Zabbix para o absolutamente necessário assim como remover o separador “overview” do menu de monitorização;
- Adicionar um novo servidor de base de dados para replicação dos dados;
- Executar um full backup a base de dados assim como a base de dados replicada;
- A medida que o sistema vai crescendo aumentar/afinar os pollers e as caches;
- Utilizar os itens de controlo interno que o sistema proporciona e implementar outros que sejam relevantes para monitorização de todo o sistema;
- Ter um sistema de gestão de configurações sólido ou um gestor de pacotes de modo que se seja capaz de implementar e gerir as configurações dos agentes, binários e scripts;

- Resolver todos os itens que não sejam suportados assim como triggers ou então desativa-los.

O documento completo com todo o estudo encontra-se em Anexo XII - Nova arquitetura Zabbix.

5 Conclusões

5.1 Resumo do relatório

Este documento descreve todo o trabalho envolvido na implementação do novo sistema de monitorização e alarmística do IPO Porto. Explica todos os passos que foram necessários efetuar e todos os requisitos e recursos utilizados para a implementação assim como todos os estudos e testes efetuados. Apresenta também todas as funcionalidades e objetivos que foram implementados e cumpridos e limitação que causaram desvios dos planos inicialmente traçados.

5.2 Objetivos realizados

Os objetivos definidos no início do projeto foram concluídos com relativo sucesso. Relativo sucesso porque, apesar de as configurações e implementações testadas e aprovadas em ambiente de testes, a transição para o ambiente de produção que se encontrava em vigor se mostrou impossível. Essa razão deveu-se a dimensão da infraestrutura do Hospital e dos poucos recursos alocados no sistema de produção, que não estavam pensados para o incremento de carga que essas novas configurações traziam.

As questões com a monitorização de todos os ativos de rede e de suporte de todos os itens considerados relevantes foram introduzidos, assim como a criação do todo o sistema alarmístico, com definição de notificações e auto-resposta aos problemas. A escalabilidade e o controlo de despoletação dos problemas foram introduzidos, assim como as questões de acesso individuais.

A disposição da informação de problemas, estudo de comportamentos e de performance e histórico foram introduzidos e simplificados permitindo leituras rápidas sem grande necessidade de execução de estudos profundos.

5.3 Outros trabalhos realizados

Todas as doenças conhecidas tem um identificador único internacional fornecendo ao pessoal médico um meio de identificação de doenças, transparente em qualquer parte do mundo. Foi então proposto a criação de um novo método de visualização e consulta da Classificação

Internacional de Doenças versão 9 (International Classification of Diseases 9). Para esta tarefa foi utilizada a aplicação Help & manual 6, que permite a criação de uma listagem de conteúdos de uma forma hierárquica, Figura 22 – Listagem hierárquica do identificador de doenças.

Classificação Internacional de Doenças 9

- 📖 IDC 9 - CM DIAGNOSTICOS
 - 📌 000 - DOENCAS INFECCIOSAS E PARASITARIAS
 - 📌 140 - TUMORES (NEOPLASIAS)
 - 📌 240 - DOENCAS ENDOCRINAS, NUTRICIONAIS, METABOLICAS E DA IMUNIDADE
 - 📌 280 - DOENCAS DO SANGUE E DOS ORGAOS HEMATOPOIETICOS
 - 📂 280 - ANEMIA POR DEFICIENCIA DE FERRO
 - 📄 2800 - ANEMIA POR DEFICIENCIA DE FERRO DEVIDA A PERDA SANGUE (CRONICA)
 - 📄 2801 - ANEMIA POR DEFICIENCIA DE FERRO SECUNDARIA A DIETA POBRE EM FERRO
 - 📄 2808 - ANEMIA POR DEFICIENCIA DE FERRO, NCOP
 - 📄 2809 - ANEMIA POR DEFICIENCIA DE FERRO, NAO ESPECIFICADA
 - 📂 281 - ANEMIAS POR DEFICIENCIA NCOP
 - 📂 282 - ANEMIAS HEMOLITICAS HEREDITARIAS
 - 📂 283 - ANEMIAS HEMOLITICAS ADQUIRIDAS
 - 📂 284 - ANEMIA APLASTICA E OUTROS SINDROMOS DE FALENCIA DA MEDULA OSSEA
 - 📂 285 - ANEMIAS NAO CLASSIFICAVEIS EM OUTRA PARTE OU NAO ESPECIFICADAS
 - 📂 286 - DEFEITOS DA COAGULACAO
 - 📂 287 - PURPURA E OUTRAS CONDICOOES HEMORRAGICAS
 - 📂 288 - DOENCAS DOS LEUCOCITOS
 - 📂 289 - DOENCAS DO SANGUE E DOS ORGAOS HEMATOPOIETICOS, NCOP
 - 📌 290 - DOENCAS MENTAIS
 - 📌 320 - DOENCAS DO SISTEMA NERVOSE E DOS ORGAOS DOS SENTIDOS
 - 📌 390 - DOENCAS DO APARELHO CIRCULATORIO
 - 📌 460 - DOENCAS DO APARELHO RESPIRATORIO
 - 📌 520 - DOENCAS DO APARELHO DIGESTIVO
 - 📌 580 - DOENCAS DO APARELHO GENITURINARIO
 - 📌 630 - COMPLICACOES DA GRAVIDEZ, DO PARTO E DO PUERPERIO
 - 📌 680 - DOENCAS DA PELE E DO TECIDO SUBCUTANEO
 - 📌 710 - DOENCAS DO APARELHO OSTEOMUSCULAR E DO TECIDO CONJUNTIVO
 - 📌 740 - ANOMALIAS CONGENITAS
 - 📌 760 - CERTAS CONDICOOES ORIGINADAS NO PERIODO PERINATAL
 - 📌 780 - SINTOMAS, SINAIS E CONDICOOES MAL DEFINIDAS
 - 📌 800 - LESOES E INTOXICACOES
 - 📌 V01 - CLASSIFICACAO SUPLEMENTAR FACTORES COM INFLUENCIA NO ESTADO DE SAUDE E CONTACTO COM SERVICO SAUDE
- 📌 IDC 9 - CM CAUSAS EXTERNAS
- 📌 IDC 9 - PCS PROCEDIMENTOS

Figura 22 – Listagem hierárquica do identificador de doenças

Esta listagem foi incorporada no portal de saúde do IPO Porto estando assim disponível para consulta por todo o pessoal.

5.4 Limitações e trabalho futuro

Ao longo da realização do projeto foram-se deparando com problemas e limitações que foram atrasando o projeto e que levaram a alteração da ideia inicial. A limitação principal deparou-se com falta de capacidade do sistema já implementado suportar as novas configurações do novo sistema. Foi necessário a elaboração de um estudo de uma arquitetura que permitisse a incorporação dessas configurações deixando espaço de manobra para futuras melhorias/funcionalidades.

Foram deixadas algumas ideias, que devido a falta de tempo e/ou recursos tiveram que ser deixadas de parte, sendo consideradas como trabalho futuro:

- Estudo, limpeza e reestruturação da monitorização/alarmística já implementada, pois foram detetados certos itens que estão duplicados, em contradição, não suportados pelos equipamentos e alguns inúteis.
- Estudo e implementação de novos itens de monitorização, e respetiva alarmística, seguindo interesse mostrado por vários elementos da equipa de informática:
- Ligar o Zabbix ao OTRS para que este, na existência de um problema, automaticamente crie um novo *ticket* para a (s) pessoa (s) devida (s).
- Estudar a possibilidade de ligação do Zabbix ao sistema do sinfNotifica na inevitabilidade de “crash” ou sistemas em baixo os utilizadores sejam notificado de um “downtime” do serviço evitando assim um contacto telefónico ou de outro tipo.
- Criação de uma página no portal onde será possível ver o estado dos vários servidores/serviços da instituição permitindo assim que o utilizador final a consulte previamente antes de efetuar o contacto com a informática.

O documento elaborado encontra-se na íntegra em Anexo XIII - Plano para desenvolvimento futuro .

5.5 Apreciação final

5.5.1 Planeamento do trabalho

O planeamento do todo o projeto foi, a meu ver, definido de uma forma correta, sendo definidos logo a partida quais os objetivos principais e secundários, sendo logo definidos também tempos de conclusão, existindo abertura de alteração desses tempo mediante problemas e situações que foram sendo deparados ao longo do tempo. A validação dos mesmos antes da passagem para uma próxima fase/tarefa também se mostrou produtiva, com a inclusão de novas ideias e alterações evitando assim os casos de ter que voltar a fases anterior consideradas como fechadas, permitindo um melhor controlo de tempo.

5.5.2 Solução

A escolha da solução, também a meu ver, mostrou-se a acertada pois revelou-se bastante intuitiva na criação e configuração de todos os elementos necessários para a implementação de todos os objetivos propostos, existindo outras funcionalidades que não sendo utilizadas, abriam portas a futuros desenvolvimentos de outros projetos.

6 Referências

- [IPO Porto, 2015a] IPO Porto - História, <http://www.ipoportor.pt/sobre/historia/>,
[último acesso: Out 2015].
- [IPO Porto, 2015b] IPO Porto – Missão, Valores e Objetivos,
<http://www.ipoportor.pt/sobre/missao-valores-e-objetivos/>,
[último acesso: Out 2015].
- [IPO Porto, 2015c] IPO Porto – Triângulo Estratégico, <http://www.ipoportor.pt/sobre/triangulo-estrategico/>,
[último acesso: Out 2015].
- [Nagios, 2015a] Nagios - History, <https://www.nagios.org/about/history/>,
[último acesso: Set 2015].
- [Nagios, 2015b] Nagios - Nagios Core Documentation,
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/toc.html/>,
[último acesso: Set 2015].
- [Pplware, 2015a] Pplware - Nágios – Monitorização Open Source,
<http://pplware.sapo.pt/tutoriais/networking/nagios-%E2%80%93-monitorizacao-open-source/>,
[último acesso: Set 2015].
- [Pplware, 2015b] Pplware - Zabbix – O próximo passo em monitorização de Redes,
<http://pplware.sapo.pt/internet/zabbix-o-proximo-passo-em-monitorizacao-de-redes/>,
[último acesso: Set 2015].
- [Wikipedia, 2015a] Wikipedia - Cacti (software),
https://en.wikipedia.org/wiki/Cacti_%28software%29,
[último acesso: Set 2015].
- [Wikipedia, 2015b] Wikipedia - Spiceworks,
<https://en.wikipedia.org/wiki/Spiceworks>,
[último acesso: Set 2015].
- [Wikipedia, 2015c] Wikipedia - Observium,
<https://en.wikipedia.org/wiki/Observium>,
[último acesso: Set 2015].
- [Wikipedia, 2015d] Wikipedia - Zabbix,
<https://en.wikipedia.org/wiki/Zabbix>,
[último acesso: Set 2015].
- [Cacti, 2015] Cacti - About Cacti,
<http://www.cacti.net/>,
[último acesso: Set 2015].
- [SpiceWorks, 2015] SpiceWorks – Apps,
<http://www.spiceworks.com/app/>,
[último acesso: Set 2015].
- [Observium, 2015] Observium - Observium Documentation,
<http://observium.org/docs/>,
[último acesso: Set 2015].
- [Zabbix, 2015] Zabbix – Documentation,
<http://www.zabbix.com/documentation.php>,
[último acesso: Set 2015].

Anexo I

Dados recolhidos da MIB do Switch

Anexo II

Dados recolhidos da MIB do Access
Point

Graph	Name	OID	Data Type	Example	Relevant?
System	sysDescr	1.3.6.1.2.1.1.1	STRING	Cisco IOS Software, C1200 Software (C1200-K9W7-M), Version 12.3(8)JEE, RELEASE SOFTWARE (fc1)	Yes
	sysObjectID	1.3.6.1.2.1.1.2	OID	1.3.6.1.4.1.9.1.525	No
	sysUpTime	1.3.6.1.2.1.1.3	Timeticks	(932774) 2:35:27.74	Yes
	sysContact	1.3.6.1.2.1.1.4	STRING	IPOP Informatica <informatica@ipopoporto.min-saude.pt>	Yes
	sysName	1.3.6.1.2.1.1.5	STRING	AccessPoint	Yes
	sysLocation	1.3.6.1.2.1.1.6	STRING	Edificio A, Piso 2	Yes
	sysServices	1.3.6.1.2.1.1.7	INTEGER	2	Yes
	sysORLastChange	1.3.6.1.2.1.1.8	Timeticks	(0) 0:00:00.00	No
Interface	ifNumber	1.3.6.1.2.1.2.1	INTEGER	6	Yes
	ifIndex	1.3.6.1.2.1.2.2.1.1	INTEGER	1	No
	ifDescr	1.3.6.1.2.1.2.2.1.2	STRING	Dot11Radio0	Yes
	ifType	1.3.6.1.2.1.2.2.1.3	INTEGER	ieee80211(71)	Yes
	ifMtu	1.3.6.1.2.1.2.2.1.4	INTEGER	1500	No
	ifSpeed	1.3.6.1.2.1.2.2.1.5	Gauge32	54000000	Yes
	ifPhysAddress	1.3.6.1.2.1.2.2.1.6	STRING	0:11:21:cc:86:30	Yes
	ifAdminStatus	1.3.6.1.2.1.2.2.1.7	INTEGER	down(2)	Yes
	ifOperStatus	1.3.6.1.2.1.2.2.1.8	INTEGER	down(2)	Yes
	ifLastChange	1.3.6.1.2.1.2.2.1.9	Timeticks	(855) 0:00:08.55	Yes
	ifInOctets	1.3.6.1.2.1.2.2.1.10	Counter32	755421	Yes
	ifInUcastPkts	1.3.6.1.2.1.2.2.1.11	Counter32	4896	Yes
	ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	Counter32	3728	Yes
	ifInDiscards	1.3.6.1.2.1.2.2.1.13	Counter32	0	Yes
	ifInErrors	1.3.6.1.2.1.2.2.1.14	Counter32	0	Yes
	ifInUnknownProtos	1.3.6.1.2.1.2.2.1.15	Counter32	22	Yes
	ifOutOctets	1.3.6.1.2.1.2.2.1.16	Counter32	1601148	Yes
	ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17	Counter32	5240	Yes
	ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18	Counter32	236	Yes
	ifOutDiscards	1.3.6.1.2.1.2.2.1.19	Counter32	0	Yes
	ifOutErrors	1.3.6.1.2.1.2.2.1.20	Counter32	0	Yes
	ifOutQLen	1.3.6.1.2.1.2.2.1.21	Gauge32	0	Yes
	ifSpecific	1.3.6.1.2.1.2.2.1.22	OID	1.2.840.10036	No
	ifName	1.3.6.1.2.1.31.1.1.1.1	STRING	Fa0	Yes
	ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2	Counter32	842	Yes
	ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3	Counter32	3728	Yes
	ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4	Counter32	227	Yes
	ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5	Counter32	9	Yes
	ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6	Counter64	749122	Yes
	ifHCInUcastPkts	1.3.6.1.2.1.31.1.1.1.7	Counter64	4825	Yes
	ifHCInMulticastPkts	1.3.6.1.2.1.31.1.1.1.8	Counter64	3721	Yes
	ifHCInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.9	Counter64	2951	Yes
	ifHCOutOctets	1.3.6.1.2.1.31.1.1.1.10	Counter64	1715358	Yes
	ifHCOutUcastPkts	1.3.6.1.2.1.31.1.1.1.11	Counter64	6043	Yes
ifHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12	Counter64	5138	Yes	
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13	Counter64	9	Yes	
ifLinkUpDownTrapEnable	1.3.6.1.2.1.31.1.1.1.14	INTEGER	enabled(1)	Yes	
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15	Gauge32	100	Yes	
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.1.16	INTEGER	false(2)	Yes	
ifConnectorPresent	1.3.6.1.2.1.31.1.1.1.17	INTEGER	true(1)	Yes	
ifAlias	1.3.6.1.2.1.31.1.1.1.18	STRING		Yes	
ifCounterDiscontinuityTime	1.3.6.1.2.1.31.1.1.1.19	Timeticks	(0) 0:00:00.00	Yes	
IP	ipForwarding	1.3.6.1.2.1.4.1	INTEGER	notForwarding(2)	Yes
	ipDefaultTTL	1.3.6.1.2.1.4.2	INTEGER	255	Yes
	ipInReceives	1.3.6.1.2.1.4.3	Counter32	6566	Yes
	ipInHdrErrors	1.3.6.1.2.1.4.4	Counter32	0	Yes
	ipInAddrErrors	1.3.6.1.2.1.4.5	Counter32	0	Yes
	ipForwDatagrams	1.3.6.1.2.1.4.6	Counter32	0	Yes
	ipInUnknownProtos	1.3.6.1.2.1.4.7	Counter32	0	Yes
	ipInDiscards	1.3.6.1.2.1.4.8	Counter32	0	Yes
	ipInDelivers	1.3.6.1.2.1.4.9	Counter32	6333	Yes
	ipOutRequests	1.3.6.1.2.1.4.10	Counter32	5153	Yes
	ipOutDiscards	1.3.6.1.2.1.4.11	Counter32	2	Yes
	ipOutNoRoutes	1.3.6.1.2.1.4.12	Counter32	0	Yes
	ipReasmTimeout	1.3.6.1.2.1.4.13	INTEGER	30 seconds	Yes
	ipReasmReqds	1.3.6.1.2.1.4.14	Counter32	0	Yes
	ipReasmOKs	1.3.6.1.2.1.4.15	Counter32	0	Yes
	ipReasmFails	1.3.6.1.2.1.4.16	Counter32	0	Yes
	ipFragOKs	1.3.6.1.2.1.4.17	Counter32	0	Yes
	ipFragFails	1.3.6.1.2.1.4.18	Counter32	0	Yes
	ipFragCreates	1.3.6.1.2.1.4.19	Counter32	0	Yes
	ipRoutingDiscards	1.3.6.1.2.1.4.23	Counter32	0	Yes

ICMP	icmpInMsgs	1.3.6.1.2.1.5.1	Counter32	2338	Yes
	icmpInErrors	1.3.6.1.2.1.5.2	Counter32	0	Yes
	icmpInDestUnreachs	1.3.6.1.2.1.5.3	Counter32	4	Yes
	icmpInTimeExcds	1.3.6.1.2.1.5.4	Counter32	0	Yes
	icmpInParmProbs	1.3.6.1.2.1.5.5	Counter32	0	Yes
	icmpInSrcQuenchs	1.3.6.1.2.1.5.6	Counter32	0	Yes
	icmpInRedirects	1.3.6.1.2.1.5.7	Counter32	0	Yes
	icmpInEchos	1.3.6.1.2.1.5.8	Counter32	2334	Yes
	icmpInEchoReps	1.3.6.1.2.1.5.9	Counter32	0	Yes
	icmpInTimestamps	1.3.6.1.2.1.5.10	Counter32	0	Yes
	icmpInTimestampReps	1.3.6.1.2.1.5.11	Counter32	0	Yes
	icmpInAddrMasks	1.3.6.1.2.1.5.12	Counter32	0	Yes
	icmpInAddrMaskReps	1.3.6.1.2.1.5.13	Counter32	0	Yes
	icmpOutMsgs	1.3.6.1.2.1.5.14	Counter32	2336	Yes
	icmpOutErrors	1.3.6.1.2.1.5.15	Counter32	0	Yes
	icmpOutDestUnreachs	1.3.6.1.2.1.5.16	Counter32	4	Yes
	icmpOutTimeExcds	1.3.6.1.2.1.5.17	Counter32	0	Yes
	icmpOutParmProbs	1.3.6.1.2.1.5.18	Counter32	0	Yes
	icmpOutSrcQuenchs	1.3.6.1.2.1.5.19	Counter32	0	Yes
	icmpOutRedirects	1.3.6.1.2.1.5.20	Counter32	0	Yes
icmpOutEchos	1.3.6.1.2.1.5.21	Counter32	0	Yes	
icmpOutEchoReps	1.3.6.1.2.1.5.22	Counter32	2334	Yes	
icmpOutTimestamps	1.3.6.1.2.1.5.23	Counter32	0	Yes	
icmpOutTimestampReps	1.3.6.1.2.1.5.24	Counter32	0	Yes	
icmpOutAddrMasks	1.3.6.1.2.1.5.25	Counter32	0	Yes	
icmpOutAddrMaskReps	1.3.6.1.2.1.5.26	Counter32	0	Yes	
TCP	tcpRtoAlgorithm	1.3.6.1.2.1.6.1	INTEGER	vanj(4)	Yes
	tcpRtoMin	1.3.6.1.2.1.6.2	INTEGER	300 milliseconds	Yes
	tcpRtoMax	1.3.6.1.2.1.6.3	INTEGER	60000 milliseconds	Yes
	tcpMaxConn	1.3.6.1.2.1.6.4	INTEGER	-1	Yes
	tcpActiveOpens	1.3.6.1.2.1.6.5	Counter32	0	Yes
	tcpPassiveOpens	1.3.6.1.2.1.6.6	Counter32	234	Yes
	tcpAttemptFails	1.3.6.1.2.1.6.7	Counter32	0	Yes
	tcpEstabResets	1.3.6.1.2.1.6.8	Counter32	0	Yes
	tcpCurrEstab	1.3.6.1.2.1.6.9	Gauge32	0	Yes
	tcpInSegs	1.3.6.1.2.1.6.10	Counter32	1684	Yes
	tcpOutSegs	1.3.6.1.2.1.6.11	Counter32	2060	Yes
	tcpRetransSegs	1.3.6.1.2.1.6.12	Counter32	0	Yes
tcpInErrs	1.3.6.1.2.1.6.14	Counter32	0	Yes	
tcpOutRsts	1.3.6.1.2.1.6.15	Counter32	18	Yes	
UDP	udpInDatagrams	1.3.6.1.2.1.7.1	Counter32	847	Yes
	udpNoPorts	1.3.6.1.2.1.7.2	Counter32	1534	Yes
	udpInErrors	1.3.6.1.2.1.7.3	Counter32	0	Yes
	udpOutDatagrams	1.3.6.1.2.1.7.4	Counter32	829	Yes
SNMP	snmpInPkts	1.3.6.1.2.1.11.1	Counter32	887	Yes
	snmpOutPkts	1.3.6.1.2.1.11.2	Counter32	869	Yes
	snmpInBadVersions	1.3.6.1.2.1.11.3	Counter32	0	Yes
	snmpInBadCommunityNames	1.3.6.1.2.1.11.4	Counter32	18	Yes
	snmpInBadCommunityUses	1.3.6.1.2.1.11.5	Counter32	0	Yes
	snmpInASNParseErrs	1.3.6.1.2.1.11.6	Counter32	0	Yes
	snmpInTooBigs	1.3.6.1.2.1.11.8	Counter32	0	Yes
	snmpInNoSuchNames	1.3.6.1.2.1.11.9	Counter32	0	Yes
	snmpInBadValues	1.3.6.1.2.1.11.10	Counter32	0	Yes
	snmpInReadOnly	1.3.6.1.2.1.11.11	Counter32	0	Yes
	snmpInGenErrs	1.3.6.1.2.1.11.12	Counter32	0	Yes
	snmpInTotalReqVars	1.3.6.1.2.1.11.13	Counter32	790	Yes
	snmpInTotalSetVars	1.3.6.1.2.1.11.14	Counter32	0	Yes
	snmpInGetRequests	1.3.6.1.2.1.11.15	Counter32	16	Yes
	snmpInGetNexts	1.3.6.1.2.1.11.16	Counter32	784	Yes
	snmpInSetRequests	1.3.6.1.2.1.11.17	Counter32	0	Yes
	snmpInGetResponses	1.3.6.1.2.1.11.18	Counter32	0	Yes
	snmpInTraps	1.3.6.1.2.1.11.19	Counter32	0	Yes
	snmpOutTooBigs	1.3.6.1.2.1.11.20	Counter32	0	Yes
	snmpOutNoSuchNames	1.3.6.1.2.1.11.21	Counter32	6	Yes
	snmpOutBadValues	1.3.6.1.2.1.11.22	Counter32	0	Yes
	snmpOutGenErrs	1.3.6.1.2.1.11.24	Counter32	0	Yes
	snmpOutGetRequests	1.3.6.1.2.1.11.25	Counter32	0	Yes
	snmpOutGetNexts	1.3.6.1.2.1.11.26	Counter32	0	Yes
	snmpOutSetRequests	1.3.6.1.2.1.11.27	Counter32	0	Yes
	snmpOutGetResponses	1.3.6.1.2.1.11.28	Counter32	810	Yes
	snmpOutTraps	1.3.6.1.2.1.11.29	Counter32	0	Yes
	snmpEnableAuthenTraps	1.3.6.1.2.1.11.30	INTEGER	disabled(2)	Yes
	snmpSilentDrops	1.3.6.1.2.1.11.31	Counter32	0	Yes
	snmpProxyDrops	1.3.6.1.2.1.11.32	Counter32	0	Yes

Extra	entPhysicalDescr	1.3.6.1.2.1.47.1.1.1.1.2	STRING	Cisco Aironet 1200 Series Access Point	Yes
	entPhysicalVendorType	1.3.6.1.2.1.47.1.1.1.1.3	OID	.1.3.6.1.4.1.9.12.3.1.10.16	No
	entPhysicalContainedIn	1.3.6.1.2.1.47.1.1.1.1.4	INTEGER	1	No
	entPhysicalClass	1.3.6.1.2.1.47.1.1.1.1.5	INTEGER	3	No
	entPhysicalParentRelPos	1.3.6.1.2.1.47.1.1.1.1.6	INTEGER	-1	No
	entPhysicalName	1.3.6.1.2.1.47.1.1.1.1.7	STRING	AP1210	Yes
	entPhysicalHardwareRev	1.3.6.1.2.1.47.1.1.1.1.8	STRING	"B0"	Yes
	entPhysicalFirmwareRev	1.3.6.1.2.1.47.1.1.1.1.9	STRING	""	Yes
	entPhysicalSoftwareRev	1.3.6.1.2.1.47.1.1.1.1.10	STRING	""	Yes
	entPhysicalSerialNum	1.3.6.1.2.1.47.1.1.1.1.11	STRING	FHK0828J0QJ	Yes
	entPhysicalMfgName	1.3.6.1.2.1.47.1.1.1.1.12	STRING	cisco	Yes
	entPhysicalModelName	1.3.6.1.2.1.47.1.1.1.1.13	STRING	AIR-AP1231G-E-K9	Yes
	entPhysicalAlias	1.3.6.1.2.1.47.1.1.1.1.14	STRING	""	No
	entPhysicalAssetID	1.3.6.1.2.1.47.1.1.1.1.15	STRING	""	No
	entPhysicalIsFRU	1.3.6.1.2.1.47.1.1.1.1.16	INTEGER	2	No
	entLogicalDescr	1.3.6.1.2.1.47.1.2.1.1.2	STRING	default logical entity for AIR-AP1231G-E-K9 platform	Yes
	entLogicalType	1.3.6.1.2.1.47.1.2.1.1.3	OID	.1.3.6.1.2.1	No
	entLogicalCommunity	1.3.6.1.2.1.47.1.2.1.1.4	STRING	private	No
	entLogicalTAddress	1.3.6.1.2.1.47.1.2.1.1.5	Hex-STRING	CO A8 24 11 00 A1	No
	entLogicalTDomain	1.3.6.1.2.1.47.1.2.1.1.6	OID	1.3.6.1.6.1.1	No
entLogicalContextEngineID	1.3.6.1.2.1.47.1.2.1.1.7	Hex-STRING	80 00 00 09 03 00 00 11 21 CC 86 30	No	
entLogicalContextName	1.3.6.1.2.1.47.1.2.1.1.8	STRING	""	No	
entLastChangeTime	1.3.6.1.2.1.47.1.4.1	Timeticks	(793) 0:00:07.93	No	

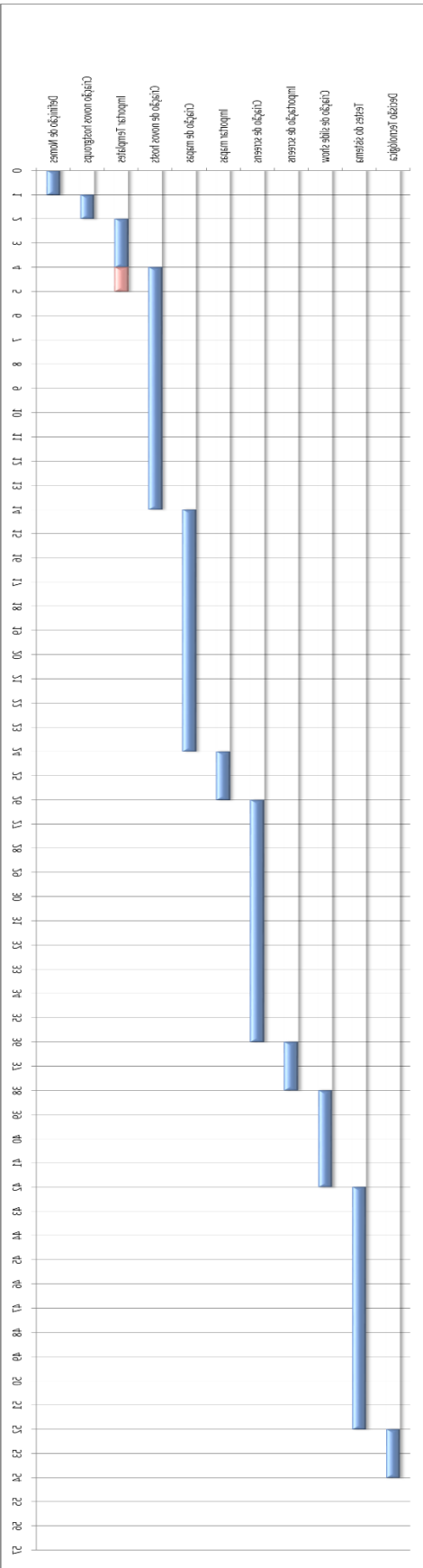
Anexo III

Dados recolhidos da MIB da UPS

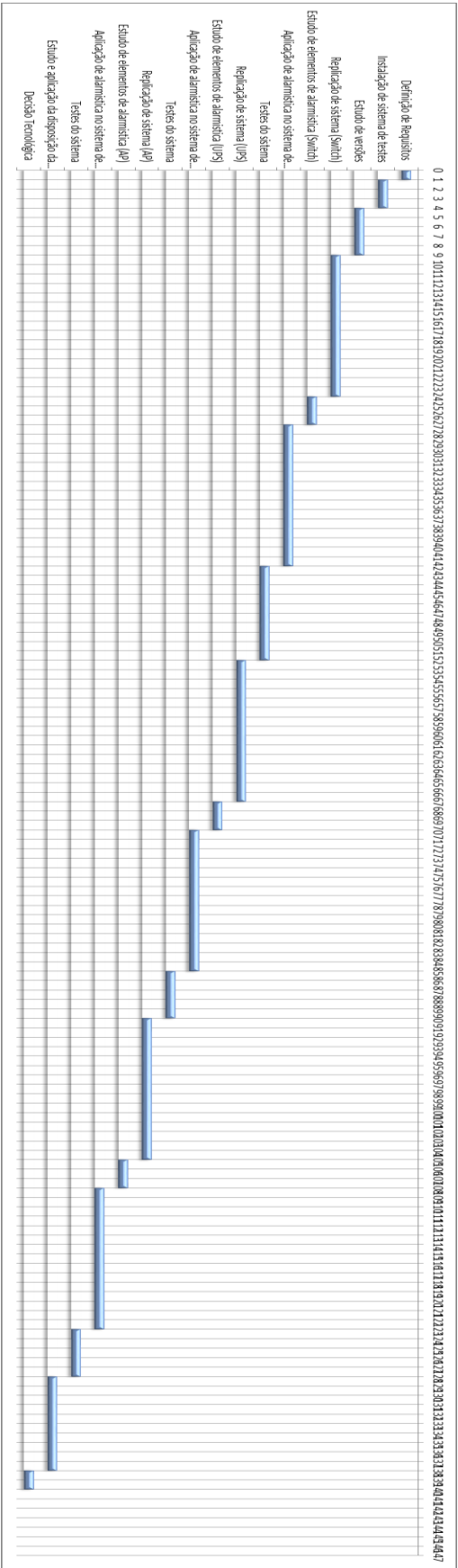
Protocol	Complete Name	Mib	Name	OID	Data Type	Example	Options	Observm	Location	Relevant?	Visualization Type
System	DISMAN-EVENT-MIB::sysUpTimeInstance	SNMPv2-MIB	sysUpTimeInstance	1.3.6.1.2.1.1.3.0	INTEGER	156831				Yes	Yes
	SNMPv2-MIB::sysDescr.0	SNMPv2-MIB	sysDescr	1.3.6.1.2.1.1.1.0	STRING	NetMan 300 : Ver. 2.02				Yes	Yes
	SNMPv2-MIB::sysContact.0	SNMPv2-MIB	sysContact	1.3.6.1.2.1.1.4.0	STRING	Informatica				Yes	Yes
	SNMPv2-MIB::sysName.0	SNMPv2-MIB	sysName	1.3.6.1.2.1.1.5.0	STRING	''				Yes	Yes
	SNMPv2-MIB::sysLocation.0	SNMPv2-MIB	sysLocation	1.3.6.1.2.1.1.6.0	STRING	Laboratorios				Yes	Yes
	SNMPv2-MIB::sysServices.0	SNMPv2-MIB	sysServices	1.3.6.1.2.1.1.7.0	INTEGER	''				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.1.1.0	SNMPv2-SMI	sysManufacturer	1.3.6.1.2.1.33.1.1.0	STRING	UPS MANUFACTURING				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.1.2.0	SNMPv2-SMI	sysModel	1.3.6.1.2.1.33.1.1.2.0	STRING	ULTXXXXXXXXXXXX				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.1.3.0	SNMPv2-SMI	sysUPSSoftwareVersion	1.3.6.1.2.1.33.1.1.3.0	Hex-STRING	5357 4D 3D 30 38 2D 30 31 2D 30 32 0D 00 00 00				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.1.4.0	SNMPv2-SMI	sysAgentSoftwareVersion	1.3.6.1.2.1.33.1.1.4.0	STRING	NetMan 300 : Ver. 2.02				Yes	Yes
SNMPv2-SMI::mib-2-33.1.1.5.0	SNMPv2-SMI	sysAlias	1.3.6.1.2.1.33.1.1.5.0	STRING	UPS_Spiso				Yes	Yes	
SNMPv2-SMI::mib-2-33.1.1.6.0	SNMPv2-SMI	sysAttachedDevices	1.3.6.1.2.1.33.1.1.6.0	Hex-STRING	00 00 00 00 00 00 00 00 00 00 00				Yes	Yes	
Interface	IF-MIB::ifNumber.0	IF-MIB	ifNumber	1.3.6.1.2.1.2.1.0	INTEGER	''				No	No
Battery	SNMPv2-SMI::mib-2-33.1.2.1.0	SNMPv2-SMI	batteryStatus	1.3.6.1.2.1.33.1.2.1.0	INTEGER	2				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.2.2.0	SNMPv2-SMI	batterySecsOnDr	1.3.6.1.2.1.33.1.2.2.0	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.2.3.0	SNMPv2-SMI	batteryEstimatedMinutesRemaining	1.3.6.1.2.1.33.1.2.3.0	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.2.4.0	SNMPv2-SMI	batteryEstimatedChargeRemaining	1.3.6.1.2.1.33.1.2.4.0	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.2.5.0	SNMPv2-SMI	batteryVoltage	1.3.6.1.2.1.33.1.2.5.0	INTEGER	274				Yes	Yes
Input	SNMPv2-SMI::mib-2-33.1.3.1.0	SNMPv2-SMI	inputLineBads	1.3.6.1.2.1.33.1.3.1.0	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.3.2.0	SNMPv2-SMI	inputNumLines	1.3.6.1.2.1.33.1.3.2.0	INTEGER	1				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.3.3.1.1	SNMPv2-SMI	inputLineIndex	1.3.6.1.2.1.33.1.3.3.1.1	INTEGER	1				No	No
	SNMPv2-SMI::mib-2-33.1.3.3.1.2	SNMPv2-SMI	inputFrequency	1.3.6.1.2.1.33.1.3.3.1.2	INTEGER	500				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.3.3.1.3	SNMPv2-SMI	inputVoltage	1.3.6.1.2.1.33.1.3.3.1.3	INTEGER	225				Yes	Yes
Output	SNMPv2-SMI::mib-2-33.1.3.3.1.4	SNMPv2-SMI	inputCurrent	1.3.6.1.2.1.33.1.3.3.1.4	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.3.3.1.5	SNMPv2-SMI	inputTruePower	1.3.6.1.2.1.33.1.3.3.1.5	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.4.1.0	SNMPv2-SMI	outputSource	1.3.6.1.2.1.33.1.4.1.0	INTEGER	3				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.4.2.0	SNMPv2-SMI	outputFrequency	1.3.6.1.2.1.33.1.4.2.0	INTEGER	300				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.4.3.0	SNMPv2-SMI	outputNumLines	1.3.6.1.2.1.33.1.4.3.0	INTEGER	1				Yes	Yes
Bypass	SNMPv2-SMI::mib-2-33.1.4.4.1.1	SNMPv2-SMI	outputLineIndex	1.3.6.1.2.1.33.1.4.4.1.1	INTEGER	1				No	No
	SNMPv2-SMI::mib-2-33.1.4.4.1.2	SNMPv2-SMI	outputVoltage	1.3.6.1.2.1.33.1.4.4.1.2	INTEGER	223				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.4.4.1.3	SNMPv2-SMI	outputCurrent	1.3.6.1.2.1.33.1.4.4.1.3	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.4.4.1.4	SNMPv2-SMI	outputPower	1.3.6.1.2.1.33.1.4.4.1.4	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.4.4.1.5	SNMPv2-SMI	outputPercentLoad	1.3.6.1.2.1.33.1.4.4.1.5	INTEGER	0				Yes	Yes
Alarm	SNMPv2-SMI::mib-2-33.1.5.1.0	SNMPv2-SMI	bypassFrequency	1.3.6.1.2.1.33.1.5.1.0	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.5.2.0	SNMPv2-SMI	bypassNumLines	1.3.6.1.2.1.33.1.5.2.0	INTEGER	1				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.5.3.1.1	SNMPv2-SMI	bypassLineIndex	1.3.6.1.2.1.33.1.5.3.1.1	INTEGER	1				No	No
	SNMPv2-SMI::mib-2-33.1.5.3.1.2	SNMPv2-SMI	bypassVoltage	1.3.6.1.2.1.33.1.5.3.1.2	INTEGER	0				Yes	Yes
	SNMPv2-SMI::mib-2-33.1.5.3.1.3	SNMPv2-SMI	bypassCurrent	1.3.6.1.2.1.33.1.5.3.1.3	INTEGER	0				Yes	Yes
Well Known Alarms	SNMPv2-SMI::mib-2-33.1.6.1.0	SNMPv2-SMI	alarmsPresent	1.3.6.1.2.1.33.1.6.1.0	INTEGER	0				No	No
	upsAlarm	upsAlarmId	1.3.6.1.2.1.33.1.6.2.11	No	No						
	upsAlarm	upsAlarmDescr	1.3.6.1.2.1.33.1.6.2.12	No	No						
	upsAlarm	upsAlarmTime	1.3.6.1.2.1.33.1.6.2.13	No	No						
	upsWellKnownAlarms	upsAlarmBatteryBad	1.3.6.1.2.1.33.1.6.3.1	No	No						
	upsWellKnownAlarms	upsAlarmBypassBad	1.3.6.1.2.1.33.1.6.3.10	No	No						
	upsWellKnownAlarms	upsAlarmOutputOffAsRequested	1.3.6.1.2.1.33.1.6.3.11	No	No						
	upsWellKnownAlarms	upsAlarmOutputOffAsRequested	1.3.6.1.2.1.33.1.6.3.12	No	No						
	upsWellKnownAlarms	upsAlarmChargeFailed	1.3.6.1.2.1.33.1.6.3.13	No	No						
	upsWellKnownAlarms	upsAlarmOutputOff	1.3.6.1.2.1.33.1.6.3.14	No	No						
	upsWellKnownAlarms	upsAlarmSystemOff	1.3.6.1.2.1.33.1.6.3.15	No	No						
	upsWellKnownAlarms	upsAlarmFanFailure	1.3.6.1.2.1.33.1.6.3.16	No	No						
	upsWellKnownAlarms	upsAlarmPowerFailure	1.3.6.1.2.1.33.1.6.3.17	No	No						
	upsWellKnownAlarms	upsAlarmGeneralFault	1.3.6.1.2.1.33.1.6.3.18	No	No						
	upsWellKnownAlarms	upsAlarmDiagnosticTestFailed	1.3.6.1.2.1.33.1.6.3.19	No	No						
	upsWellKnownAlarms	upsAlarmOnBattery	1.3.6.1.2.1.33.1.6.3.20	No	No						
	upsWellKnownAlarms	upsAlarmCommunicationLost	1.3.6.1.2.1.33.1.6.3.21	No	No						
	upsWellKnownAlarms	upsAlarmWaitingPower	1.3.6.1.2.1.33.1.6.3.22	No	No						
	upsWellKnownAlarms	upsAlarmShutdownPending	1.3.6.1.2.1.33.1.6.3.23	No	No						
	upsWellKnownAlarms	upsAlarmShutdownImminent	1.3.6.1.2.1.33.1.6.3.24	No	No						
	upsWellKnownAlarms	upsAlarmTestInProgress	1.3.6.1.2.1.33.1.6.3.25	No	No						
upsWellKnownAlarms	upsAlarmLowBattery	1.3.6.1.2.1.33.1.6.3.3	No	No							
upsWellKnownAlarms	upsAlarmDepletedBattery	1.3.6.1.2.1.33.1.6.3.4	INTEGER	0	No	No					
upsWellKnownAlarms	upsAlarmTempBad	1.3.6.1.2.1.33.1.6.3.5	No	No	No	No					
upsWellKnownAlarms	upsAlarmInputBad	1.3.6.1.2.1.33.1.6.3.6	No	No	No	No					
upsWellKnownAlarms	upsAlarmOutputBad	1.3.6.1.2.1.33.1.6.3.7	No	No	No	No					
upsWellKnownAlarms	upsAlarmOutputOverload	1.3.6.1.2.1.33.1.6.3.8	No	No	No	No					
upsWellKnownAlarms	upsAlarmOnBypass	1.3.6.1.2.1.33.1.6.3.9	INTEGER	1	No	No					
Test	upsTest	upsTestId	1.3.6.1.2.1.33.1.7.1	No	No						
	upsTest	upsTestSpinLock	1.3.6.1.2.1.33.1.7.2	No	No						
	upsTest	upsTestResultsSummary	1.3.6.1.2.1.33.1.7.3	No	No						
	upsTest	upsTestResultsDetail	1.3.6.1.2.1.33.1.7.4	No	No						
	upsTest	upsTestStartTime	1.3.6.1.2.1.33.1.7.5	INTEGER	0	No	No				
	upsTest	upsTestElapsedTime	1.3.6.1.2.1.33.1.7.6	No	No	No	No				
	upsTest	upsWellKnownTests	1.3.6.1.2.1.33.1.7.7	No	No	No	No				
	upsTest	upsTestNoTestsInitiated	1.3.6.1.2.1.33.1.7.7.1	No	No	No	No				
	upsTest	upsTestAbortTestInProgress	1.3.6.1.2.1.33.1.7.7.2	No	No	No	No				
	upsTest	upsTestEmergencySystemTest	1.3.6.1.2.1.33.1.7.7.3	INTEGER	0	Yes	Yes				
	upsTest	upsTestQuickBatteryTest	1.3.6.1.2.1.33.1.7.7.4	INTEGER	0	No	No				
upsTest	upsTestDeepBatteryCalibration	1.3.6.1.2.1.33.1.7.7.5	INTEGER	0	No	No					
Control	upsControl	upsShutdownType	1.3.6.1.2.1.33.1.8.1	No	No						
	upsControl	upsShutdownAlarmDelay	1.3.6.1.2.1.33.1.8.2	INTEGER	0	No	No				
	upsControl	upsStartupAlertDelay	1.3.6.1.2.1.33.1.8.3	INTEGER	0	No	No				
	upsControl	upsRebootWithDuration	1.3.6.1.2.1.33.1.8.4	INTEGER	0	No	No				
Config	upsControl	upsAutoRestart	1.3.6.1.2.1.33.1.8.5	INTEGER	0	No	No				
	SNMPv2-SMI::mib-2-33.1.9.1.0	SNMPv2-SMI	configInputVoltage	1.3.6.1.2.1.33.1.9.1.0	INTEGER	0	Yes	Yes			
	SNMPv2-SMI::mib-2-33.1.9.2.0	SNMPv2-SMI	configInputFreq	1.3.6.1.2.1.33.1.9.2.0	INTEGER	0	Yes	Yes			
	SNMPv2-SMI::mib-2-33.1.9.3.0	SNMPv2-SMI	configOutputVoltage	1.3.6.1.2.1.33.1.9.3.0	INTEGER	0	Yes	Yes			
	SNMPv2-SMI::mib-2-33.1.9.4.0	SNMPv2-SMI	configOutputFreq	1.3.6.1.2.1.33.1.9.4.0	INTEGER	0	Yes	Yes			
	SNMPv2-SMI::mib-2-33.1.9.5.0	SNMPv2-SMI	configOutputVA	1.3.6.1.2.1.33.1.9.5.0	INTEGER	0	Yes	Yes			
	SNMPv2-SMI::mib-2-33.1.9.6.0	SNMPv2-SMI	configOutputPower	1.3.6.1.2.1.33.1.9.6.0	INTEGER	0	Yes	Yes			
	SNMPv2-SMI::mib-2-33.1.9.7.0	SNMPv2-SMI	configConfigLowBatTime	1.3.6.1.2.1.33.1.9.7.0	INTEGER	0	Yes	Yes			
SNMPv2-SMI::mib-2-33.1.9.8.0	SNMPv2-SMI	configConfigAudiibleStatus	1.3.6.1.2.1.33.1.9.8.0	INTEGER	0	Yes	Yes				
SNMPv2-SMI::mib-2-33.1.9.9.0	SNMPv2-SMI	configConfigLowVoltageTransferPoint	1.3.6.1.2.1.33.1.9.9.0	INTEGER	0	Yes	Yes				
SNMPv2-SMI::mib-2-33.1.9.10.0	SNMPv2-SMI	configConfigHighVoltageTransferPoint	1.3.6.1.2.1.33.1.9.10.0	INTEGER	0	Yes	Yes				
Traps	upsTraps	upsTrapOnBattery	1.3.6.1.2.1.33.2.1	No	No	No	No				
	upsTraps	upsTrapTestCompleted	1.3.6.1.2.1.33.2.2	No	No	No	No				
	upsTraps	upsTrapAlarmEntryRemoved	1.3.6.1.2.1.33.2.3	No	No	No	No				
Conformance	upsCompliances	upsSubsetCompliance	1.3.6.1.2.1.33.3.1.1	No	No	No	No				
	upsCompliances	upsBasicCompliance	1.3.6.1.2.1.33.3.1.2	No	No	No	No				
	upsCompliances	upsFullCompliance	1.3.6.1.2.1.33.3.1.3	No	No	No	No				
Conformance-Subsets	upsSubsets	upsSubsetIdentifierGroup	1.3.6.1.2.1.33.3.2.1	No	No	No	No				
	upsSubsets	upsSubsetBatteryGroup	1.3.6.1.2.1.33.3.2.1.2	No	No	No	No				
	upsSubsets	upsSubsetInputGroup	1.3.6.1.2.1.33.3.2.1.3	No	No	No	No				
	upsSubsets	upsSubsetOutputGroup	1.3.6.1.2.1.33.3.2.1.4	No	No	No	No				
	upsSubsets	upsSubsetAlarmGroup	1.3.6.1.2.1.33.3.2.1.6	No	No	No	No				
	upsSubsets	upsSubsetControlGroup	1.3.6.1.2.1.33.3.2.1.8	No	No	No	No				
	upsSubsets	upsSubsetConfigGroup	1.3.6.1.2.1.33.3.2.1.9	No	No	No	No				
Conformance-Groups	upsBasicGroups	upsBasicIdentifierGroup	1.3.6.1.2.1.33.3.2.2.1	No	No	No	No				
	upsBasicGroups	upsBasicBatteryGroup	1.3.6.1.2.1.33.3.2.2.2	No	No	No	No				
	upsBasicGroups	upsBasicInputGroup	1.3.6.1.2.1.33.3.2.2.3	No	No	No	No				
	upsBasicGroups	upsBasicOutputGroup	1.3.6.1.2.1.33.3.2.2.4	No	No	No	No				
	upsBasicGroups	upsBasicBypassGroup	1.3.6.1.2.1.33.3.2.2.5	No	No	No	No				
	upsBasicGroups	upsBasicAlarmGroup	1.3.6.1.2.1.33.3.2.2.6	No	No	No	No				
	upsBasicGroups	upsBasicTestGroup	1.3.6.1.2.1.33.3.2.2.7	No	No	No	No				
Conformance-Groups	upsBasicGroups	upsBasicControlGroup	1.3.6.1.2.1.33.3.2.2.8	No	No	No	No				
	upsBasicGroups	upsBasicConfigGroup	1.3.6.1.2.1.33.3.2.2.9	No	No	No	No				
	upsFullGroups	upsFullIdentifierGroup	1.3.6.1.2.1.33.3.2.3.1	No	No	No	No				
	upsFullGroups	upsFullBatteryGroup	1.3.6.1.2.1.33.3.2.3.2	No	No	No	No				
	upsFullGroups	upsFullInputGroup	1.3.6.1.2.1.33.3.2.3.3	No	No	No	No				
	upsFullGroups	upsFullOutputGroup	1.3.6.1.2.1.33.3.2.3.4	No	No	No	No				
Conformance-Groups	upsFullGroups	upsFullBypassGroup	1.3.6.1.2.1.33.3.2.3.5	No	No	No	No				
	upsFullGroups	upsFullAlarmGroup	1.3.6.1.2.1.33.3.2.3.6	No	No	No	No				
	upsFullGroups	upsFullTestGroup	1.3.6.1.2.1.33.3.2.3.7	No	No	No	No				
	upsFullGroups	upsFullControlGroup	1.3.6.1.2.1.33.3.2.3.8	No	No	No	No				
	upsFullGroups	upsFullConfigGroup	1.3.6.1.2.1.33.3.2.3.9	No	No	No	No				

Anexo IV

Mapas de Gant



Fase de produção



Fase de desenvolvimento

Anexo V

Estudo integral do Switch

Graphs	Name	Type	Key	SNMP OID	Type of Information	Units	Update Interval [sec]	History Storage Period (day)	Trends Storage Period (day)	Store value	Multiplier	Check?
SYSTEM	SYSTEMUptime	SNMPv2-agent	sys.UptimeInstance	1.3.6.1.2.1.1.3.0	Numeric(Decimal)	uptime	1 Minute (60)	90	365	As is	0.01	No
	SYSTEMDescription	SNMPv2-agent	sys.Descri	1.3.6.1.2.1.1.1.0	Text		24 Hours (86400)	90		History (Chassis)		No
	SYSTEMName	SNMPv2-agent	sys.Name	1.3.6.1.2.1.1.5.0	Text		24 Hours (86400)	90		History (Name)		No
	SYSTEMContact	SNMPv2-agent	sys.Contact	1.3.6.1.2.1.1.4.0	Text		24 Hours (86400)	90		History (Contact)		No
	SYSTEMLocation	SNMPv2-agent	sys.Location	1.3.6.1.2.1.1.4.0	Text		24 Hours (86400)	90		History (Location)		No
	SYSTEMHardware	SNMPv2-agent	mb-2.47.1.1.1.1.8.2	1.3.6.1.2.1.47.1.1.1.1.8.2	Text		24 Hours (86400)	90		History (Hardware)		No
	SYSTEMOSVersion	SNMPv2-agent	mb-2.47.1.1.1.1.10.2	1.3.6.1.2.1.47.1.1.1.1.10.2	Text		24 Hours (86400)	90		History (OS)		No
	SYSTEMModel	SNMPv2-agent	mb-2.47.1.1.1.1.13.2	1.3.6.1.2.1.47.1.1.1.1.13.2	Text		24 Hours (86400)	90		History (Model)		No
	SYSTEMVendor	SNMPv2-agent	mb-2.47.1.1.1.1.12.2	1.3.6.1.2.1.47.1.1.1.1.12.2	Text		24 Hours (86400)	90		History (Vendor)		No
	SYSTEMSerialNumber	SNMPv2-agent	mb-2.47.1.1.1.1.11.2	1.3.6.1.2.1.47.1.1.1.1.11.2	Text		24 Hours (86400)	90		History (Serial number A)		No
	SYSTEMFirmware	SNMPv2-agent	mb-2.47.1.1.1.1.9.2	1.3.6.1.2.1.47.1.1.1.1.9.2	Text		24 Hours (86400)	90		History (Software)		No
ICMP Statistics	ICMP InMsgs	SNMPv2-agent	icmp.inMsgs	1.3.6.1.2.1.5.1.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP OutMsgs	SNMPv2-agent	icmp.outMsgs	1.3.6.1.2.1.5.1.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP InErrors	SNMPv2-agent	icmp.inErrors	1.3.6.1.2.1.5.2.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP OutErrors	SNMPv2-agent	icmp.outErrors	1.3.6.1.2.1.5.2.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP InEchoes	SNMPv2-agent	icmp.inEchoes	1.3.6.1.2.1.5.8.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP OutEchoes	SNMPv2-agent	icmp.outEchoes	1.3.6.1.2.1.5.8.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP InEchoReps	SNMPv2-agent	icmp.inEchoReps	1.3.6.1.2.1.5.9.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP OutEchoReps	SNMPv2-agent	icmp.outEchoReps	1.3.6.1.2.1.5.9.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP InSrcQuenches	SNMPv2-agent	icmp.inSrcQuenches	1.3.6.1.2.1.5.22.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP OutSrcQuenches	SNMPv2-agent	icmp.outSrcQuenches	1.3.6.1.2.1.5.22.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP InRedirects	SNMPv2-agent	icmp.inRedirects	1.3.6.1.2.1.5.19.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
ICMP Informational Statistics	ICMP InRedirects	SNMPv2-agent	icmp.inRedirects	1.3.6.1.2.1.5.20.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP InAddrMasks	SNMPv2-agent	icmp.inAddrMasks	1.3.6.1.2.1.5.20.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP InAddrMaskReps	SNMPv2-agent	icmp.inAddrMaskReps	1.3.6.1.2.1.5.25.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP OutAddrMasks	SNMPv2-agent	icmp.outAddrMasks	1.3.6.1.2.1.5.25.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	ICMP OutAddrMaskReps	SNMPv2-agent	icmp.outAddrMaskReps	1.3.6.1.2.1.5.30.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	IP ForwDatagrams	SNMPv2-agent	ip.ForwDatagrams	1.3.6.1.2.1.4.6.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	IP InDelivers	SNMPv2-agent	ip.InDelivers	1.3.6.1.2.1.4.9.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	IP InReceives	SNMPv2-agent	ip.InReceives	1.3.6.1.2.1.4.3.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	IP OutRequests	SNMPv2-agent	ip.OutRequests	1.3.6.1.2.1.4.10.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	IP InDiscards	SNMPv2-agent	ip.InDiscards	1.3.6.1.2.1.4.8.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	IP OutDiscards	SNMPv2-agent	ip.OutDiscards	1.3.6.1.2.1.4.11.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
IP OutRoutes	SNMPv2-agent	ip.OutRoutes	1.3.6.1.2.1.4.12.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No	
IP FragOKs	SNMPv2-agent	ip.FragOKs	1.3.6.1.2.1.4.17.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No	
IP ReasmOKs	SNMPv2-agent	ip.ReasmOKs	1.3.6.1.2.1.4.15.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No	
IP ReasmFails	SNMPv2-agent	ip.ReasmFails	1.3.6.1.2.1.4.16.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No	
IP FragCreates	SNMPv2-agent	ip.FragCreates	1.3.6.1.2.1.4.19.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No	
IP ReasmReqs	SNMPv2-agent	ip.ReasmReqs	1.3.6.1.2.1.4.14.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No	
SNMP Statistics	SNMP InTraps	SNMPv2-agent	snmp.inTraps	1.3.6.1.2.1.11.39.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	SNMP InTotalReqVars	SNMPv2-agent	snmp.inTotalReqVars	1.3.6.1.2.1.11.13.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	SNMP InTotalSetVars	SNMPv2-agent	snmp.inTotalSetVars	1.3.6.1.2.1.11.14.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	SNMP OutTraps	SNMPv2-agent	snmp.outTraps	1.3.6.1.2.1.11.29.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	SNMP OutGetResponses	SNMPv2-agent	snmp.outGetResponses	1.3.6.1.2.1.11.28.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	SNMP OutSetRequests	SNMPv2-agent	snmp.outSetRequests	1.3.6.1.2.1.11.27.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
SNMP Packet Type Statistics	SNMP InPKts	SNMPv2-agent	snmp.inPKts	1.3.6.1.2.1.11.1.0	Numeric(float)	PKts	1 Minute (60)	90	365	Delta (speed per second)		No
	SNMP OutPKts	SNMPv2-agent	snmp.outPKts	1.3.6.1.2.1.11.2.0	Numeric(float)	PKts	1 Minute (60)	90	365	Delta (speed per second)		No
TCP Statistics	TCP InSegs	SNMPv2-agent	tcp.inSegs	1.3.6.1.2.1.6.10.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	TCP OutSegs	SNMPv2-agent	tcp.outSegs	1.3.6.1.2.1.6.11.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	TCP ActiveOpens	SNMPv2-agent	tcp.activeOpens	1.3.6.1.2.1.6.5.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	TCP PassiveOpens	SNMPv2-agent	tcp.passiveOpens	1.3.6.1.2.1.6.6.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	TCP AttemptFails	SNMPv2-agent	tcp.attemptFails	1.3.6.1.2.1.6.7.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	TCP EstabResets	SNMPv2-agent	tcp.estabResets	1.3.6.1.2.1.6.8.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
UDP Statistics	TCP RetransSegs	SNMPv2-agent	tcp.retransSegs	1.3.6.1.2.1.6.12.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	UDP InDatagrams	SNMPv2-agent	udp.inDatagrams	1.3.6.1.2.1.7.1.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	UDP OutDatagrams	SNMPv2-agent	udp.outDatagrams	1.3.6.1.2.1.7.4.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	UDP InErrors	SNMPv2-agent	udp.inErrors	1.3.6.1.2.1.7.3.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
INTERFACE	UDP NoPorts	SNMPv2-agent	udp.noPorts	1.3.6.1.2.1.7.2.0	Numeric(float)		1 Minute (60)	90	365	Delta (speed per second)		No
	IF Number 0	SNMPv2-agent	if.Number0	1.3.6.1.2.1.2.1.0	Text	uptime	1 Hour (3600)	90	365	As is	0.01	No
INTERFACE	IF InLastChange 0	SNMPv2-agent	if.InLastChange0	1.3.6.1.2.1.3.11.5.0	Numeric(Decimal)	uptime	1 Hour (3600)	90	365	As is	0.01	No
	IF StackLastChange 0	SNMPv2-agent	if.StackLastChange0	1.3.6.1.2.1.3.11.6.0	Numeric(Decimal)	uptime	1 Hour (3600)	90	365	As is	0.01	No

Graphs	Name	Type	Key	SNMP OID	Type of Information	Units	Update Interval (sec)	History storage period (day)	Trends storage period (day)	Store/Show value	Multiplier	Check?
Traffic	IF InOctets.22	SNMPv2 agent	IF.InOctets.22	.1.3.6.1.2.1.2.1.10.22	Numeric(Float)	Bits/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF OutOctets.22	SNMPv2 agent	IF.OutOctets.22	.1.3.6.1.2.1.2.1.16.22	Numeric(Float)	Bits/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF HcInOctets.22	SNMPv2 agent	IF.HcInOctets.22	.1.3.6.1.2.1.31.1.1.6.22	Numeric(Float)	Bits/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF HcOutOctets.22	SNMPv2 agent	IF.HcOutOctets.22	.1.3.6.1.2.1.31.1.1.10.22	Numeric(Float)	Bits/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF TotalOutOctets.22	SNMPv2 agent	IF.TotalOutOctets.22	.1.3.6.1.2.1.2.1.16.22	Text		1 Hour (3600)	90			No	No
	IF TotalInOctets.22	SNMPv2 agent	IF.TotalInOctets.22	.1.3.6.1.2.1.2.1.10.22	Text		1 Hour (3600)	90			No	No
	IF InUnicastPkts.22	SNMPv2 agent	IF.InUnicastPkts.22	.1.3.6.1.2.1.2.1.11.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF OutUnicastPkts.22	SNMPv2 agent	IF.OutUnicastPkts.22	.1.3.6.1.2.1.2.1.17.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
Unicast Packets	IF HcInUnicastPkts.22	SNMPv2 agent	IF.HcInUnicastPkts.22	.1.3.6.1.2.1.31.1.1.1.722	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF HcOutUnicastPkts.22	SNMPv2 agent	IF.HcOutUnicastPkts.22	.1.3.6.1.2.1.31.1.1.11.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF InBroadcastPkts.22	SNMPv2 agent	IF.InBroadcastPkts.22	.1.3.6.1.2.1.31.1.1.1.5.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF OutBroadcastPkts.22	SNMPv2 agent	IF.OutBroadcastPkts.22	.1.3.6.1.2.1.31.1.1.1.5.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF HcInBroadcastPkts.22	SNMPv2 agent	IF.HcInBroadcastPkts.22	.1.3.6.1.2.1.31.1.1.1.9.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF HcOutBroadcastPkts.22	SNMPv2 agent	IF.HcOutBroadcastPkts.22	.1.3.6.1.2.1.31.1.1.1.13.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF InMulticastPkts.22	SNMPv2 agent	IF.InMulticastPkts.22	.1.3.6.1.2.1.2.1.11.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF OutMulticastPkts.22	SNMPv2 agent	IF.OutMulticastPkts.22	.1.3.6.1.2.1.2.1.18.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
Non Unicast Packets	IF InMulticastPkts.22	SNMPv2 agent	IF.InMulticastPkts.22	.1.3.6.1.2.1.31.1.1.1.7.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF OutMulticastPkts.22	SNMPv2 agent	IF.OutMulticastPkts.22	.1.3.6.1.2.1.31.1.1.1.7.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF HcInMulticastPkts.22	SNMPv2 agent	IF.HcInMulticastPkts.22	.1.3.6.1.2.1.31.1.1.1.4.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF HcOutMulticastPkts.22	SNMPv2 agent	IF.HcOutMulticastPkts.22	.1.3.6.1.2.1.31.1.1.1.8.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF InErrors.22	SNMPv2 agent	IF.InErrors.22	.1.3.6.1.2.1.2.1.14.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF OutErrors.22	SNMPv2 agent	IF.OutErrors.22	.1.3.6.1.2.1.2.1.20.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF InDiscards.22	SNMPv2 agent	IF.InDiscards.22	.1.3.6.1.2.1.2.1.13.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF OutDiscards.22	SNMPv2 agent	IF.OutDiscards.22	.1.3.6.1.2.1.2.1.19.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
Unknown Protocols	IF InUnknownProtos.22	SNMPv2 agent	IF.InUnknownProtos.22	.1.3.6.1.2.1.2.1.15.22	Numeric(Decimal)	Pkts/s	1 Minute (60)	90	365	Delta (speed per second)	No	No
	IF Name.22	SNMPv2 agent	IF.Name.22	.1.3.6.1.2.1.31.1.1.1.1.22	Text		24 Hours (86400)	90			No	No
	IF Descr.22	SNMPv2 agent	IF.Descr.22	.1.3.6.1.2.1.2.1.2.22	Text		24 Hours (86400)	90			No	No
	IF Type.22	SNMPv2 agent	IF.Type.22	.1.3.6.1.2.1.2.1.3.22	Character		24 Hours (86400)	90		Media	No	No
	IF Speed.22	SNMPv2 agent	IF.Speed.22	.1.3.6.1.2.1.2.1.5.22	Text		24 Hours (86400)	90			No	No
	IF Alias.22	SNMPv2 agent	IF.Alias.22	.1.3.6.1.2.1.31.1.1.18.22	Text		24 Hours (86400)	90			No	No
	IF HighSpeed.22	SNMPv2 agent	IF.HighSpeed.22	.1.3.6.1.2.1.31.1.1.15.22	Text		24 Hours (86400)	90			No	No
	IF AdminStatus.22	SNMPv2 agent	IF.AdminStatus.22	.1.3.6.1.2.1.2.1.17.22	Character		1 Hour (3600)/1 Minute (60)	90		SNMP interface status (AdminStatus)	No	No
IF OperStatus.22	SNMPv2 agent	IF.OperStatus.22	.1.3.6.1.2.1.2.1.8.22	Character		1 Hour (3600)/1 Minute (60)	90		SNMP interface status (OperStatus)	No	No	
Interface	IF LastChange.22	SNMPv2 agent	IF.LastChange.22	.1.3.6.1.2.1.2.1.9.22	Numeric(Decimal)	uptime	1 Hour (3600)	90		365	As is	0.01
	IF LinkUpDownTrapEnable.22	SNMPv2 agent	IF.LinkUpDownTrapEnable.22	.1.3.6.1.2.1.31.1.1.1.4.22	Character		1 Minute (60)	90		Link Up Down Trap Enable	No	No
	IF PromiscuousMode.22	SNMPv2 agent	IF.PromiscuousMode.22	.1.3.6.1.2.1.31.1.1.1.16.22	Character		1 Minute (60)	90		Mode Status	No	No
	IF ConnectorPresent.22	SNMPv2 agent	IF.ConnectorPresent.22	.1.3.6.1.2.1.31.1.1.1.17.22	Character		24 Hours (86400)	90		Mode Status	No	No
	IF CounterDiscontinuityTime.22	SNMPv2 agent	IF.CounterDiscontinuityTime.22	.1.3.6.1.2.1.31.1.1.1.19.22	Numeric(Decimal)	uptime	1 Hour (3600)	90		365	As is	0.01
	IF StackStatus.0.22	SNMPv2 agent	IF.StackStatus.0.22		Stack		1 Hour (3600)	90		Row Status	No	No
	IF StackStatus.22.0	SNMPv2 agent	IF.StackStatus.22.0		Stack		1 Hour (3600)	90		Row Status	No	No

Graphs	Name	Type	Key	SNMP OID	Type of Information	Units	Update Interval (sec)	History storage period (day)	Trends storage period (day)	Store/Show value	Multiplier	Check?
EtherLike	EtherLike StatsIndex.22	SNMPv2-agent	EtherLike.StatsIndex.22	.1.3.6.1.2.1.10.7.2.1.1.22	Text	Errors	24 Hours (86400)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsAlignmentErrors.22	SNMPv2-agent	EtherLike.StatsAlignmentErrors.22	.1.3.6.1.2.1.10.7.2.1.1.2.22	Numeric(Decimal)	Errors	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsCSErrors.22	SNMPv2-agent	EtherLike.StatsCSErrors.22	.1.3.6.1.2.1.10.7.2.1.1.3.22	Numeric(Decimal)	Errors	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsSingleCollisionFrames.22	SNMPv2-agent	EtherLike.StatsSingleCollisionFrames.22	.1.3.6.1.2.1.10.7.2.1.1.4.22	Numeric(Decimal)	Collisions	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsMultipleCollisionFrames.22	SNMPv2-agent	EtherLike.StatsMultipleCollisionFrames.22	.1.3.6.1.2.1.10.7.2.1.1.5.22	Numeric(Decimal)	Collisions	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsSQETestErrors.22	SNMPv2-agent	EtherLike.StatsSQETestErrors.22	.1.3.6.1.2.1.10.7.2.1.1.6.22	Numeric(Decimal)	Errors	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsDeferredTransmissions.22	SNMPv2-agent	EtherLike.StatsDeferredTransmissions.22	.1.3.6.1.2.1.10.7.2.1.1.7.22	Numeric(Decimal)	Collisions	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsLateCollisions.22	SNMPv2-agent	EtherLike.StatsLateCollisions.22	.1.3.6.1.2.1.10.7.2.1.1.8.22	Numeric(Decimal)	Collisions	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsExcessiveCollisions.22	SNMPv2-agent	EtherLike.StatsExcessiveCollisions.22	.1.3.6.1.2.1.10.7.2.1.1.9.22	Numeric(Decimal)	Collisions	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsInternalMacTransmitErrors.22	SNMPv2-agent	EtherLike.StatsInternalMacTransmitErrors.22	.1.3.6.1.2.1.10.7.2.1.1.10.22	Numeric(Decimal)	Errors	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsCarrierSenseErrors.22	SNMPv2-agent	EtherLike.StatsCarrierSenseErrors.22	.1.3.6.1.2.1.10.7.2.1.1.11.22	Numeric(Decimal)	Errors	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherLike StatsFrameTooLong.22	SNMPv2-agent	EtherLike.StatsFrameTooLong.22	.1.3.6.1.2.1.10.7.2.1.1.12.22	Numeric(Decimal)	Errors	1 Minute (60)	90	90	365 Delta (simple change)	No	No
EtherLike StatsInternalMacReceiveErrors.22	SNMPv2-agent	EtherLike.StatsInternalMacReceiveErrors.22	.1.3.6.1.2.1.10.7.2.1.1.16.22	Numeric(Decimal)	Errors	1 Minute (60)	90	90	365 Delta (simple change)	No	No	

Graphs	Name	Type	Key	SNMP OID	Type of Information	Units	Update Interval (sec)	History storage period (day)	Trends storage period (day)	Store/Show value	Multiplier	Check?
EtherStats Info	EtherStats Index.22	SNMPv2-agent	etherStats.Index.22	.1.3.6.1.2.1.16.1.1.1.1.1.22	Text	Errors	24 Hours (86400)	90	90	Entry Status	No	No
	EtherStats Status.22	SNMPv2-agent	etherStats.Status.22	.1.3.6.1.2.1.16.1.1.1.1.21.22	Character	Errors	1 Hour (3600)	90	90	Entry Status	No	No
	EtherStats Owner.22	SNMPv2-agent	etherStats.Owner.22	.1.3.6.1.2.1.16.1.1.1.1.20.22	Text	Errors	1 Hour (3600)	90	90	Entry Status	No	No
EtherStats Traffic	EtherStats Octets.22	SNMPv2-agent	etherStats.Octets.22	.1.3.6.1.2.1.16.1.1.1.1.4.22	Numeric(Decimal)	Octets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Pkts.22	SNMPv2-agent	etherStats.Pkts.22	.1.3.6.1.2.1.16.1.1.1.1.5.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats BroadcastPkts.22	SNMPv2-agent	etherStats.BroadcastPkts.22	.1.3.6.1.2.1.16.1.1.1.1.6.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Fragments.22	SNMPv2-agent	etherStats.Fragments.22	.1.3.6.1.2.1.16.1.1.1.1.11.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats MulticastPkts.22	SNMPv2-agent	etherStats.MulticastPkts.22	.1.3.6.1.2.1.16.1.1.1.1.7.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
EtherStats Errors	EtherStats CRCAlignErrors.22	SNMPv2-agent	etherStats.CRCAlignErrors.22	.1.3.6.1.2.1.16.1.1.1.1.8.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats DropEvents.22	SNMPv2-agent	etherStats.DropEvents.22	.1.3.6.1.2.1.16.1.1.1.1.3.22	Numeric(Decimal)	Drops	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Jabbers.22	SNMPv2-agent	etherStats.Jabbers.22	.1.3.6.1.2.1.16.1.1.1.1.12.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Collisions.22	SNMPv2-agent	etherStats.Collisions.22	.1.3.6.1.2.1.16.1.1.1.1.13.22	Numeric(Decimal)	Collisions	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats OversizePkts.22	SNMPv2-agent	etherStats.OversizePkts.22	.1.3.6.1.2.1.16.1.1.1.1.10.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
EtherStats Packets Size	EtherStats UndersizePkts.22	SNMPv2-agent	etherStats.UndersizePkts.22	.1.3.6.1.2.1.16.1.1.1.1.9.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Pkts64Octets.22	SNMPv2-agent	etherStats.Pkts64Octets.22	.1.3.6.1.2.1.16.1.1.1.1.1.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Pkts65to127Octets.22	SNMPv2-agent	etherStats.Pkts65to127Octets.22	.1.3.6.1.2.1.16.1.1.1.1.2.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Pkts128to255Octets.22	SNMPv2-agent	etherStats.Pkts128to255Octets.22	.1.3.6.1.2.1.16.1.1.1.1.16.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Pkts256to511Octets.22	SNMPv2-agent	etherStats.Pkts256to511Octets.22	.1.3.6.1.2.1.16.1.1.1.1.17.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
EtherStats Packets Size	EtherStats Pkts512to1023Octets.22	SNMPv2-agent	etherStats.Pkts512to1023Octets.22	.1.3.6.1.2.1.16.1.1.1.1.18.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No
	EtherStats Pkts1024to15180Octets.22	SNMPv2-agent	etherStats.Pkts1024to15180Octets.22	.1.3.6.1.2.1.16.1.1.1.1.19.22	Numeric(Decimal)	Packets	1 Minute (60)	90	90	365 Delta (simple change)	No	No

Anexo VI

Estudo completo da alarmística do
Switch

Graphs	Name	Necessary?	Trigger Name	Trigger Fire	Severity	Expression	Message	Depends	Check?
SYSTEM	SYSTEM Uptime	Yes	Switch Down (3 Minutes)	Immediately (0) 3 Minutes (300)	Warning	(24 Ports Device sys.UpTimeInstance.moddata(300)=1 & (24 Ports Device sys.UpTimeInstance.moddata(180))=1 & (24 Ports Device sys.UpTimeInstance.moddata(180))=1 & (24 Ports Device sys.UpTimeInstance.moddata(180))=1)	Switch (HOSTNAME) is Down! Switch (HOSTNAME) didn't boot up! Switch (HOSTNAME) is Down! for too long!!	Switch Down (3 Minutes) & Switch Down (1 Hour)	No
	SYSTEM Description	No	Switch Down (1 Hour)	1 Hour (3600)	Disaster	(24 Ports Device sys.UpTimeInstance.moddata(3600))=1 & (24 Ports Device sys.UpTimeInstance.moddata(0))=1)			No
	SYSTEM Name	No							No
	SYSTEM Contact	No							No
	SYSTEM Location	No							No
	SYSTEM Firmware	No							No
	SYSTEM Version	No							No
	SYSTEM Model	No							No
	SYSTEM Vendor	No							No
	SYSTEM Serial Number	No							No
ICMP Statistics	ICMP InMsgs	No							No
	ICMP OutMsgs	No							No
	ICMP In Errors	Yes	ICMP In Errors	+10 errors for 5 minutes (300)	Warning	(24 Ports Device icmp.InErrors.last(300))>10 & (24 Ports Device icmp.InErrors.last(60))>10	Switch (HOSTNAME) is reporting too many In Errors!		No
	ICMP Out Errors	Yes	ICMP Out Errors	+10 errors for 5 minutes (300)	Warning	(24 Ports Device icmp.OutErrors.last(300))>10 & (24 Ports Device icmp.OutErrors.last(60))>10	Switch (HOSTNAME) is reporting too many Out Errors!		No
	ICMP In Echoes	No							No
	ICMP Out Echoes	No							No
	ICMP In Echoes	No							No
	ICMP In Echoes	No							No
	ICMP In Echoes	No							No
	ICMP In Echoes	No							No
ICMP Informational Statistics	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
	ICMP InRequests	No							No
IP Statistics	IP Forwarded	No							No
	IP Forwarded	No							No
	IP InDelivers	No							No
	IP InDelivers	No							No
	IP InReceives	No							No
	IP InReceives	No							No
	IP OutRequests	No							No
	IP OutRequests	No							No
	IP OutDiscards	No							No
	IP OutDiscards	No							No
IP Fragmentation Statistics	IP OutNoRoutes	No							No
	IP FragOKs	No							No
	IP FragFalls	No							No
	IP ReasmOKs	No							No
	IP ReasmOKs	No							No
	IP ReasmFalls	No							No
	IP FragCreates	No							No
	IP FragCreates	No							No
	IP FragCreates	No							No
	IP FragCreates	No							No
SNMP Statistics	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
	SNMP InTraps	No							No
SNMP Packet Type Statistics	SNMP InPKTs	No							No
	SNMP InPKTs	No							No
	SNMP OutPKTs	No							No
	SNMP OutPKTs	No							No
	TCP InSegs	No							No
	TCP OutSegs	No							No
	TCP ActiveOpens	No							No
	TCP ActiveOpens	No							No
	TCP PassiveOpens	No							No
	TCP AttemptFails	No							No
UDP Statistics	TCP EstablishResets	No							No
	TCP RetransSegs	No							No
	UDP InDatagrams	No							No
	UDP InDatagrams	No							No
	UDP InErrors	Yes	UDP In Errors	+10 errors for 5 minutes (300)	Warning	(24 Ports Device udp.InErrors.last(300))>10 & (24 Ports Device udp.InErrors.last(60))>10	Switch (HOSTNAME) is reporting too many In Errors!		No
	UDP NoPorts	Yes	UDP No Ports	+10 errors for 5 minutes (300)	Warning	(24 Ports Device udp.NoPorts.last(300))>10 & (24 Ports Device udp.NoPorts.last(60))>10	Switch (HOSTNAME) is reporting too many No Ports!		No
	IF Number 0	No							No
	IF Statuses Change 0	No							No
	IF Statuses Change 0	No							No
	INTERFACE								

Graphs	Name	Necessary?	Trigger Name	Trigger Fire	Severity	Expression	Message	Depends	Check?
Traffic	IF InOctets.22	No							No
	IF OutOctets.22	No							No
	IF HcinOctets.22	No							No
	IF HcoutOctets.22	No							No
	IF TotalOutOctets.22	No							No
	IF TotalInOctets.22	No							No
Unicast Packets	IF InUcastPkts.22	No							No
	IF OutUcastPkts.22	No							No
	IF HcinUcastPkts.22	No							No
	IF HcoutUcastPkts.22	No							No
	IF InBroadcastPkts.22	No							No
	IF OutBroadcastPkts.22	No							No
Non Unicast Packets	IF HcinBroadcastPkts.22	No							No
	IF HcoutBroadcastPkts.22	No							No
	IF InUcastPkts.22	No							No
	IF OutUcastPkts.22	No							No
	IF InMulticastPkts.22	No							No
	IF OutMulticastPkts.22	No							No
	IF HcinMulticastPkts.22	No							No
	IF HcoutMulticastPkts.22	No							No
	IF InErrors.22	Yes	Port 22 - In Errors	+10 errors for 5 minutes (300)	Warning	{Port 22:if.InErrors.22.last(.300)}>10 & {Port 22:if.InErrors.22.last(#2)}>10	Switch {HOSTNAME} Port 22 It's reporting too many In Errors!		No
	IF OutErrors.22	Yes	Port 22 - Out Errors	+10 errors for 5 minutes (300)	Warning	{Port 22:if.OutErrors.22.last(.300)}>10 & {Port 22:if.OutErrors.22.last(#2)}>10	Switch {HOSTNAME} Port 22 It's reporting too many Out Errors!		No
IF InDiscards.22	Yes	Port 22 - In Discards	+10 errors for 5 minutes (300)	Warning	{Port 22:if.InDiscards.22.last(.300)}>10 & {Port 22:if.InDiscards.22.last(#2)}>10	Switch {HOSTNAME} Port 22 It's reporting too many In Discards!		No	
IF OutDiscards.22	Yes	Port 22 - Out Discards	+10 errors for 5 minutes (300)	Warning	{Port 22:if.OutDiscards.22.last(.300)}>10 & {Port 22:if.OutDiscards.22.last(#2)}>10	Switch {HOSTNAME} Port 22 It's reporting too many Out Discards!		No	
Unknown Protocols	IF InUnknownProtos.22	Yes	Port 22 - In Unknown Protos	+10 errors for 5 minutes (300)	Warning	{Port 22:if.InUnknownProtos.22.last(.300)}>10 & {Port 22:if.InUnknownProtos.22.last(#2)}>10	Switch {HOSTNAME} Port 22 It's reporting too many in Unknown Protos!		No
Interface	IF Name.22	No							No
	IF Descr.22	No							No
	IF Type.22	No							No
	IF Speed.22	No							No
	IF Alias.22	No							No
	IF HighSpeed.22	No							No
	IF AdminStatus.22	No	Port 22 - Admin Status	Immediately (0)	Average	{Port 22:if.AdminStatus.22.last(.60)}=2 & {Port 22:if.AdminStatus.22.last()}=2	Switch {HOSTNAME} Port 22 Admin Status it's Down!		No
	IF OperStatus.22	Yes	Port 22 - Oper Status	5 Minutes (300)	Warning	{Port 22:if.OperStatus.22.last(.300)}=2 & {Port 22:if.OperStatus.22.last()}=2	Switch {HOSTNAME} Port 22 Oper Status it's Down for too long!		No
	IF LastChange.22	No							No
	IF LinkUpDownTrapEnable.22	No							No
IF PromiscuousMode.22	No							No	
IF ConnectorPresent.22	No							No	
IF CounterDiscontinuityTime.22	No							No	
IF StackStatus.0.22	No								No
IF StackStatus.22.0	No								No

Graphs	Name	Necessary?	Trigger Name	Trigger Fire	Severity	Expression	Message	Depends	Check?
EtherLike	EtherLike StatsIndex.22	No							No
	EtherLike StatsAlignmentErrors.22	Yes	Port 22 - Alignment Errors	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsAlignmentErrors.22.last(.300))>10 & (Port 22:EtherLike.StatsAlignmentErrors.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Alignment Errors!		No
	EtherLike StatsFCSErrors.22	Yes	Port 22 - FCS Errors	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsFCSErrors.22.last(.300))>10 & (Port 22:EtherLike.StatsFCSErrors.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many FCS Errors!		No
	EtherLike StatsSingleCollisionFrames.22	Yes	Port 22 - Single Collision Frames	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsSingleCollisionFrames.22.last(.300))>10 & (Port 22:EtherLike.StatsSingleCollisionFrames.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Single Collision Frames!		No
	EtherLike StatsMultipleCollisionFrames.22	Yes	Port 22 - Multiple Collision Frames	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsMultipleCollisionFrames.22.last(.300))>10 & (Port 22:EtherLike.StatsMultipleCollisionFrames.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Multiple Collision Frames!		No
	EtherLike StatsSQTTestErrors.22	Yes	Port 22 - SQT Test Errors	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsSQTTestErrors.22.last(.300))>10 & (Port 22:EtherLike.StatsSQTTestErrors.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many SQT Test Errors!		No
	EtherLike StatsDeferredTransmissions.22	Yes	Port 22 - Deferred Transmissions	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsDeferredTransmissions.22.last(.300))>10 & (Port 22:EtherLike.StatsDeferredTransmissions.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Deferred Transmissions!		No
	EtherLike StatsLateCollisions.22	Yes	Port 22 - Late Collisions	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsLateCollisions.22.last(.300))>10 & (Port 22:EtherLike.StatsLateCollisions.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Late Collisions!		No
	EtherLike StatsExcessiveCollisions.22	Yes	Port 22 - Excessive Collisions	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsExcessiveCollisions.22.last(.300))>10 & (Port 22:EtherLike.StatsExcessiveCollisions.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Excessive Collisions!		No
	EtherLike StatsInternalMacTransmitErrors.22	Yes	Port 22 - Internal Mac Transmit Errors	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsInternalMacTransmitErrors.22.last(.300))>10 & (Port 22:EtherLike.StatsInternalMacTransmitErrors.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Internal Mac Transmit Errors!		No
	EtherLike StatsCarrierSenseErrors.22	Yes	Port 22 - Carrier Sense Errors	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsCarrierSenseErrors.22.last(.300))>10 & (Port 22:EtherLike.StatsCarrierSenseErrors.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Carrier Sense Errors!		No
	EtherLike StatsFrameTooLong.22	Yes	Port 22 - Frame Too Long	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsFrameTooLong.22.last(.300))>10 & (Port 22:EtherLike.StatsFrameTooLong.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Frame Too Longs!		No
EtherLike StatsInternalMacReceiveErrors.22	Yes	Port 22 - Internal Mac Receive Errors	+10 errors for 5 minutes (300)	Warning	((Port 22:EtherLike.StatsInternalMacReceiveErrors.22.last(.300))>10 & (Port 22:EtherLike.StatsInternalMacReceiveErrors.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Internal Mac Receive Errors!		No	

Graphs	Name	Necessary?	Trigger Name	Trigger Fire	Severity	Expression	Message	Depends	Check?
EtherStats Info	EtherStats Index.22	No							No
	EtherStats Status.22	No							No
	EtherStats Owner.22	No							No
EtherStats	EtherStats Pkts.22	No							No
	EtherStats BroadcastPkts.22	No							No
	EtherStats Fragments.22	No							No
EtherStats Traffic	EtherStats MulticastPkts.22	No							No
	EtherStats CRCAlignErrors.22	Yes	Port 22 - CRC Align Errors	+10 errors for 5 minutes (300)	Warning	((Port 22:etherStats.CRCAlignErrors.22.last(.300))>10 & (Port 22:etherStats.CRCAlignErrors.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many CRC Align Errors!		No
	EtherStats DropEvents.22	Yes	Port 22 - Drop Events	+10 errors for 5 minutes (300)	Warning	((Port 22:etherStats.DropEvents.22.last(.300))>10 & (Port 22:etherStats.DropEvents.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Drop Events!		No
	EtherStats Jabbers.22	No							No
	EtherStats Collisions.22	Yes	Port 22 - Collisions	+10 errors for 5 minutes (300)	Warning	((Port 22:etherStats.Collisions.22.last(.300))>10 & (Port 22:etherStats.Collisions.22.last(#2))>10)	Switch [HOSTNAME] Port 22 It's reporting too many Collisions!		No
EtherStats Packets Size	EtherStats OversizePkts.22	No							No
	EtherStats UndersizePkts.22	No							No
	EtherStats Pkts64Octets.22	No							No
	EtherStats Pkts65to127Octets.22	No							No
	EtherStats Pkts128to255Octets.22	No							No
	EtherStats Pkts256to511Octets.22	No							No
EtherStats Pkts512to1023Octets.22	No							No	
EtherStats Pkts1024to15183Octets.22	No							No	

Anexo VII

Estudo integral da UPS

Graphs	Name	Type	Key	SNMP OID	Type of Information	Units	Update Interval (sec)	History Storage Period (day)	Trends Storage Period (day)	Store/Show Value	Multiplier	Check?
SYSTEM	SYSTEM Uptime	SNMPV1 agent	sys.Uptime	1.3.6.1.2.1.1.3.0	Numeric(Decimal)	uptime	1 Minute (60)	90	365	As Is	0.01	No
	SYSTEM Description	SNMPV1 agent	sys.Descr	1.3.6.1.2.1.1.1.0	Text		24 Hours (86400)	90		History (Chassis)		No
	SYSTEM Contact	SNMPV1 agent	sys.Contact	1.3.6.1.2.1.1.4.0	Text		24 Hours (86400)	90		History (Contact)		No
	SYSTEM Name	SNMPV2 agent	sys.Name	1.3.6.1.2.1.1.5.0	Text		24 Hours (86400)	90		History (Name)		No
	SYSTEM Location	SNMPV1 agent	sys.Location	1.3.6.1.2.1.1.6.0	Text		24 Hours (86400)	90		History (Location)		No
	SYSTEM Services	SNMPV1 agent	sys.Services	1.3.6.1.2.1.1.7.0	Text		24 Hours (86400)	90		History (Software application A)		No
	SYSTEM Manufacturer	SNMPV1 agent	sys.Manufacturer	1.3.6.1.2.1.3.1.1.1.0	Text		24 Hours (86400)	90		History (Vendor)		No
	SYSTEM Model	SNMPV1 agent	sys.Model	1.3.6.1.2.1.3.1.1.2.0	Text		24 Hours (86400)	90		History (Model)		No
	SYSTEM UPS Software Version	SNMPV1 agent	sys.UPSSoftwareVersion	1.3.6.1.2.1.3.3.1.1.3.0	Text		24 Hours (86400)	90		History (OS)		No
	SYSTEM Agent Software Version	SNMPV1 agent	sys.AgentSoftwareVersion	1.3.6.1.2.1.3.3.1.1.4.0	Text		24 Hours (86400)	90		History (Software)		No
SYSTEM Alias	SNMPV1 agent	sys.Alias	1.3.6.1.2.1.3.3.1.1.5.0	Text		24 Hours (86400)	90		History (Name)		No	
SYSTEM Attached Devices	SNMPV1 agent	sys.AttachedDevices	1.3.6.1.2.1.3.3.1.1.6.0	Text		24 Hours (86400)	90		History (Notes)		No	
Battery	BATTERY Status	SNMPV1 agent	battery.Status	1.3.6.1.2.1.3.3.1.2.1.0	Character		5 Minutes (300)	90		APC Battery Status		No
	BATTERY Voltage	SNMPV1 agent	battery.Voltage	1.3.6.1.2.1.3.3.1.2.5.0	Numeric(Float)	Volts	1 Minute (60)	90	365	As Is	0.1	No
Battery Times	BATTERY Current	SNMPV1 agent	battery.Current	1.3.6.1.2.1.3.3.1.2.6.0	Numeric(Decimal)	Amps	1 Minute (60)	90	365	As Is	1	No
	BATTERY Temperature	SNMPV1 agent	battery.Temperature	1.3.6.1.2.1.3.3.1.2.7.0	Numeric(Float)	Amps	1 Minute (60)	90	365	As Is	1	No
Battery Times	BATTERY Seconds On Battery	SNMPV1 agent	battery.SecondsOnBattery	1.3.6.1.2.1.3.3.1.2.2.0	Numeric(Decimal)	uptime	2 Minutes (120)	90	365	As Is	0.01	No
	BATTERY Estimated Minutes Remaining	SNMPV1 agent	battery.EstimatedMinutesRemaining	1.3.6.1.2.1.3.3.1.2.3.0	Numeric(Decimal)	%	2 Minutes (120)	90	365	As Is	0.01	No
Input	BATTERY Estimated Charge Remaining	SNMPV1 agent	battery.EstimatedChargeRemaining	1.3.6.1.2.1.3.3.1.2.4.0	Numeric(Decimal)	%	2 Minutes (120)	90	365	As Is	0.01	No
	INPUT Line Bids	SNMPV1 agent	input.LineBids	1.3.6.1.2.1.3.3.1.3.1.0	Numeric(Decimal)		1 Minute (60)	90	365	Delta (simple change)		No
Output	OUTPUT Num Lines	SNMPV1 agent	output.NumLines	1.3.6.1.2.1.3.3.1.3.2.0	Text	Hertz	1 Hour (3600)	90				No
	INPUT Frequency	SNMPV1 agent	input.Frequency	1.3.6.1.2.1.3.3.1.3.1.2.1	Numeric(Float)	Hertz	1 Minute (60)	90	365	As Is	0.1	No
	INPUT Voltage	SNMPV1 agent	input.Voltage	1.3.6.1.2.1.3.3.1.3.1.3.1	Numeric(Float)	Volts	1 Minute (60)	90	365	As Is	1	No
	INPUT Current	SNMPV1 agent	input.Current	1.3.6.1.2.1.3.3.1.3.1.4.1	Numeric(Float)	Amps	1 Minute (60)	90	365	As Is	1	No
	INPUT True Power	SNMPV1 agent	input.TruePower	1.3.6.1.2.1.3.3.1.3.1.5.1	Numeric(Float)	Watts	1 Minute (60)	90	365	As Is	1	No
	OUTPUT Source	SNMPV1 agent	output.Source	1.3.6.1.2.1.3.3.1.4.1.0	Character		1 Hour (3600)	90		Output Source		No
	OUTPUT Frequency	SNMPV1 agent	output.Frequency	1.3.6.1.2.1.3.3.1.4.2.0	Numeric(Float)	Hertz	1 Minute (60)	90	365	As Is	0.1	No
	OUTPUT Num Lines	SNMPV1 agent	output.NumLines	1.3.6.1.2.1.3.3.1.4.3.0	Text		1 Hour (3600)	90				No
	OUTPUT Voltage	SNMPV1 agent	output.Voltage	1.3.6.1.2.1.3.3.1.4.4.1.2.1	Numeric(Float)	Volts	1 Minute (60)	90	365	As Is	1	No
	OUTPUT Current	SNMPV1 agent	output.Current	1.3.6.1.2.1.3.3.1.4.4.1.3.1	Numeric(Float)	Amps	1 Minute (60)	90	365	As Is	1	No
Bypass	OUTPUT Power	SNMPV1 agent	output.Power	1.3.6.1.2.1.3.3.1.4.4.1.4.1	Numeric(Float)	Watts	1 Minute (60)	90	365	As Is	1	No
	OUTPUT Percent Load	SNMPV1 agent	output.PercentLoad	1.3.6.1.2.1.3.3.1.4.4.1.5.1	Numeric(Float)	%	1 Minute (60)	90	365	As Is	1	No
Bypass	BYPASS Frequency	SNMPV1 agent	bypass.Frequency	1.3.6.1.2.1.3.3.1.5.1.0	Numeric(Float)	Hertz	1 Minute (60)	90	365	As Is	0.1	No
	BYPASS Num Lines	SNMPV1 agent	bypass.NumLines	1.3.6.1.2.1.3.3.1.5.2.0	Text		1 Hour (3600)	90				No
	BYPASS Voltage	SNMPV1 agent	bypass.Voltage	1.3.6.1.2.1.3.3.1.5.3.1.2.1	Numeric(Float)	Volts	1 Minute (60)	90	365	As Is	1	No
	BYPASS Current	SNMPV1 agent	bypass.Current	1.3.6.1.2.1.3.3.1.5.3.1.3.1	Numeric(Float)	Amps	1 Minute (60)	90	365	As Is	1	No
CONFIG	BYPASS Power	SNMPV1 agent	bypass.Power	1.3.6.1.2.1.3.3.1.5.3.1.4.1	Numeric(Float)	Watts	1 Minute (60)	90	365	As Is	1	No
	CONFIG Input Voltage	SNMPV1 agent	config.InputVoltage	1.3.6.1.2.1.3.3.1.9.1.0	Numeric(Float)	Volts	24 Hours (86400)	90	365	As Is	1	No
	CONFIG Input Freq	SNMPV1 agent	config.InputFreq	1.3.6.1.2.1.3.3.1.9.2.0	Numeric(Float)	Hertz	24 Hours (86400)	90	365	As Is	0.1	No
	CONFIG Output Voltage	SNMPV1 agent	config.OutputVoltage	1.3.6.1.2.1.3.3.1.9.3.0	Numeric(Float)	Volts	24 Hours (86400)	90	365	As Is	1	No
	CONFIG Output Freq	SNMPV1 agent	config.OutputFreq	1.3.6.1.2.1.3.3.1.9.4.0	Numeric(Float)	Hertz	24 Hours (86400)	90	365	As Is	0.1	No
	CONFIG Output VA	SNMPV1 agent	config.OutputVA	1.3.6.1.2.1.3.3.1.9.5.0	Numeric(Float)	Volts-Amps	24 Hours (86400)	90	365	As Is	1	No
	CONFIG Output Power	SNMPV1 agent	config.OutputPower	1.3.6.1.2.1.3.3.1.9.6.0	Numeric(Float)	Watts	24 Hours (86400)	90	365	As Is	1	No
	CONFIG Low Batt Time	SNMPV1 agent	config.LowBattTime	1.3.6.1.2.1.3.3.1.9.7.0	Numeric(Float)	uptime	24 Hours (86400)	90	365	As Is	0.01	No
	CONFIG Audible Status	SNMPV1 agent	config.AudibleStatus	1.3.6.1.2.1.3.3.1.9.8.0	Character		24 Hours (86400)	90		Audible Status		No
	CONFIG Low Voltage Transfer Point	SNMPV1 agent	config.LowVoltageTransferPoint	1.3.6.1.2.1.3.3.1.9.9.0	Character		24 Hours (86400)	90	365	As Is	1	No
CONFIG High Voltage Transfer Point	SNMPV1 agent	config.HighVoltageTransferPoint	1.3.6.1.2.1.3.3.1.9.10.0	Numeric(Float)		24 Hours (86400)	90	365	As Is	1	No	

Anexo VIII

Estudo completo da alarmística da UPS

Groups	Name	Necessary?	Trigger Name	Trigger Fire	Severity	Expression	Message	Depends	Checks?	
System	SYSTEM Uptime	No							No	
	SYSTEM Description	No							No	
	SYSTEM Contact	No							No	
	SYSTEM Name	No							No	
	SYSTEM Location	No							No	
	SYSTEM Manufacturer	No							No	
	SYSTEM Model	No							No	
	SYSTEM UPS Software Version	No							No	
	SYSTEM Agent Software Version	No							No	
	SYSTEM Attached Devices	No							No	
Battery	Battery Status	Yes	Battery Low Battery Depleted	Immediately (0) Immediately (0)	Warning High	(UPS.Battery.Status.Last(180))=3 & (UPS.Battery.Status.Last(180))=4 (UPS.Battery.Status.Last(180))=4 (UPS.Battery.Status.Last(180))=4 (UPS.Battery.Secondary.Battery.Last(180))=30 & (UPS.Battery.Secondary.Battery.Last(180))=40 (UPS.Battery.Secondary.Battery.Last(180))=40 & (UPS.Battery.Secondary.Battery.Last(180))=40	UPS (HOSTNAME) is Low UPS (HOSTNAME) is Depleted Device is on Battery Power! Device is on Battery Power for 3 Minutes! Device is on Battery Power for 30 Minutes!!!	Battery Depleted Device on Battery (10 Minutes) & Device on Battery (5 Minutes) Device on Battery (10 Minutes)	No	
	Battery Seconds On Battery	Yes	Device On Battery (5 Minutes) Device On Battery (10 Minutes)	Immediately (0) On for 5 minutes (300) On for 10 minutes (600)	Information Warning High	(UPS.Battery.Secondary.Battery.Last(180))=30 & (UPS.Battery.Secondary.Battery.Last(180))=40 (UPS.Battery.Secondary.Battery.Last(180))=40 & (UPS.Battery.Secondary.Battery.Last(180))=40 (UPS.Battery.Secondary.Battery.Last(180))=40 & (UPS.Battery.Secondary.Battery.Last(180))=40	Device is on Battery Power for 30 Minutes! Device is on Battery Power for 30 Minutes!!!		No	
	Battery Estimated Minutes Remaining	Yes	15 Minutes of Battery Left 10 Minutes of Battery Left 5 Minutes of Battery Left 1 Minute of Battery Left	Immediately (0) Immediately (0) Immediately (0) Immediately (0)	Warning Average High Disaster	(UPS.Battery.Secondary.Battery.Last(180))=500 (UPS.Battery.Secondary.Battery.Last(180))=600 (UPS.Battery.Secondary.Battery.Last(180))=600 & (UPS.Battery.Secondary.Battery.Last(180))=600 (UPS.Battery.Secondary.Battery.Last(180))=600 & (UPS.Battery.Secondary.Battery.Last(180))=600	10 Minutes of Battery Left & 30 Minutes of Battery Left & 1 Minute of Battery Left 5 Minutes of Battery Left & 1 Minute of Battery Left 1 Minute of Battery Left		No	
	Battery Estimated Charge Remaining	Yes	Battery Not Fully Charged	Immediately (0)	Information	(UPS.Battery.EstimateChargeRemaining.Last(180))=100 & (UPS.Battery.EstimateChargeRemaining.Last(180))=100	UPS (HOSTNAME) have 1 Minute of Battery left!!! UPS (HOSTNAME) is not fully charged!		No	
	Battery Voltage	Yes	Battery Voltage Too High	BV1 > 230 for 2 minutes (120)	Warning	(UPS.Battery.Voltage.Last(120))=250 & (UPS.Battery.Voltage.Last(120))=250	UPS (HOSTNAME) Battery Voltage is Too High!		No	
	Battery Current	Yes	Battery Current Too High	BCur > 4 for 2 minutes (120)	Warning	(UPS.Battery.Current.Last(120))=4 & (UPS.Battery.Current.Last(120))=4	UPS (HOSTNAME) Battery Current is Too High!		No	
	Battery Temperature	Yes	Battery Temperature Too High Battery Temperature Too High (300) Battery Temperature Too High (15 Minutes)	Temp > 60K for 5 minutes (300) Temp > 60K for 15 minutes (900)	Warning Warning High	(UPS.Battery.Temperature.Last(180))=50 & (UPS.Battery.Temperature.Last(180))=50 (UPS.Battery.Temperature.Last(180))=50 & (UPS.Battery.Temperature.Last(180))=50 (UPS.Battery.Temperature.Last(180))=50 & (UPS.Battery.Temperature.Last(180))=50	Battery Temperature Too High! Battery Temperature Too High (15 Minutes)		No	
	Input	Input Line Bids	Yes	Input Too Many Line Bids	InputBid > 5	Warning	(UPS.Input.LineBids.Last(180))=5	UPS (HOSTNAME) have too many Input Lines Bids!		No
		Input Num Lines	No							No
		Input Frequency	Yes	Input Frequency Too High	Freq > 60 for 2 minutes (120)	Warning	(UPS.Input.Frequency.Last(120))=600 & (UPS.Input.Frequency.Last(120))=600	UPS (HOSTNAME) Input Frequency is Too High!		No
		Input Voltage	Yes	Input Voltage Too High	V1 > 275 for 2 minutes (120)	Warning	(UPS.Input.Voltage.Last(120))=275 & (UPS.Input.Voltage.Last(120))=275	UPS (HOSTNAME) Input Voltage is Too High!		No
		Input Current	Yes	Input Current Too High	ICur > 4 for 2 minutes (120)	Warning	(UPS.Input.Current.Last(120))=4 & (UPS.Input.Current.Last(120))=4	UPS (HOSTNAME) Input Current is Too High!		No
		Output Source	No							No
Output Frequency		Yes	Output Frequency Too High	OFreq > 60 for 2 minutes (120)	Warning	(UPS.Output.Frequency.Last(120))=600 & (UPS.Output.Frequency.Last(120))=600	UPS (HOSTNAME) Output Frequency is Too High!		No	
Output Num Lines		No							No	
Output Voltage		Yes	Output Voltage Too High	OV1 > 235 for 2 minutes (120)	Warning	(UPS.Output.Voltage.Last(120))=235 & (UPS.Output.Voltage.Last(120))=235	UPS (HOSTNAME) Output Voltage is Too High!		No	
Output Current		Yes	Output Current Too High	OCur > 4 for 2 minutes (120)	Warning	(UPS.Output.Current.Last(120))=4 & (UPS.Output.Current.Last(120))=4	UPS (HOSTNAME) Output Current is Too High!		No	
Output	Output Power	Yes	Output Power Too High	OPwr > 50 for 2 minutes (120)	Warning	(UPS.Output.Power.Last(120))=500 & (UPS.Output.Power.Last(120))=500	UPS (HOSTNAME) Output Power is Too High!		No	
	Output Percent Load	Yes	Output Percent Load Too High	PLoad > 90 for 2 minutes (120)	Warning	(UPS.Output.PercentLoad.Last(120))=90 & (UPS.Output.PercentLoad.Last(120))=90	UPS (HOSTNAME) Input Percent Load is Too High!		No	
	Bypass Frequency	Yes	Bypass Frequency Too High	BFreq > 60 for 2 minutes (120)	Warning	(UPS.Bypass.Frequency.Last(120))=600 & (UPS.Bypass.Frequency.Last(120))=600	UPS (HOSTNAME) Bypass Frequency is Too High!		No	
	Bypass Num Lines	No							No	
Bypass	Bypass Voltage	Yes	Bypass Voltage Too High	BV1 > 230 for 2 minutes (120)	Warning	(UPS.Bypass.Voltage.Last(120))=230 & (UPS.Bypass.Voltage.Last(120))=230	UPS (HOSTNAME) Bypass Voltage is Too High!		No	
	Bypass Current	Yes	Bypass Current Too High	BCur > 4 for 2 minutes (120)	Warning	(UPS.Bypass.Current.Last(120))=4 & (UPS.Bypass.Current.Last(120))=4	UPS (HOSTNAME) Bypass Current is Too High!		No	
	Bypass Power	Yes	Bypass Power Too High	BPwr > 50 for 2 minutes (120)	Warning	(UPS.Bypass.Power.Last(120))=500 & (UPS.Bypass.Power.Last(120))=500	UPS (HOSTNAME) Bypass Power is Too High!		No	
	Bypass Power	No							No	
Alarm	Alarms Present	No							No	
	Alarm Time	No							No	
Config	Config Input Voltage	No							No	
	Config Output Voltage	No							No	
	Config Transfer Point	No							No	
	Config Input Freq	No							No	
	Config Output Voltage	No							No	
	Config Output Freq	No							No	
	Config Output VA	No							No	
Config	Config Output Power	No							No	
	Config Output Power	No							No	
	Config Available Status	No							No	
	Config Low Voltage Transfer Point	No							No	
	Config Low Voltage Transfer Point	No							No	

Anexo IX

Estudo integral do Access Point

ICMP Time Statistics	ICMP InTimeExcds	SNMPV2 agent	icmp.InTimeExcds	1.3.6.1.2.1.5.4.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	ICMP OutTimeExcds	SNMPV2 agent	icmp.OutTimeExcds	1.3.6.1.2.1.5.7.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	ICMP InTimeStamps	SNMPV2 agent	icmp.InTimeStamps	1.3.6.1.2.1.5.10.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	ICMP OutTimeStamps	SNMPV2 agent	icmp.OutTimeStamps	1.3.6.1.2.1.5.23.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	ICMP InTimeStampReps	SNMPV2 agent	icmp.InTimeStampReps	1.3.6.1.2.1.5.11.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	ICMP OutTimeStampReps	SNMPV2 agent	icmp.OutTimeStampReps	1.3.6.1.2.1.5.24.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	TCP Statistics	TCP InSegs	SNMPV2 agent	tcp.InSegs	1.3.6.1.2.1.6.10.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		TCP OutSegs	SNMPV2 agent	tcp.OutSegs	1.3.6.1.2.1.6.11.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		TCP ActiveOpens	SNMPV2 agent	tcp.ActiveOpens	1.3.6.1.2.1.6.5.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		TCP PassiveOpens	SNMPV2 agent	tcp.PassiveOpens	1.3.6.1.2.1.6.6.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		TCP AttemptFails	SNMPV2 agent	tcp.AttemptFails	1.3.6.1.2.1.6.7.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		TCP EstabResets	SNMPV2 agent	tcp.EstabResets	1.3.6.1.2.1.6.8.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
TCP CurrEstab		SNMPV2 agent	tcp.CurrEstab	1.3.6.1.2.1.6.9.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
TCP RetransSegs		SNMPV2 agent	tcp.RetransSegs	1.3.6.1.2.1.6.12.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
TCP RtoAlgorithm		SNMPV2 agent	tcp.RtoAlgorithm	1.3.6.1.2.1.6.1.0	Character	1 Hour (3600)	90	Algorithm Used	No	
TCP RtoMin		SNMPV2 agent	tcp.RtoMin	1.3.6.1.2.1.6.2.0	Text	1 Hour (3600)	90		No	
TCP RtoMax		SNMPV2 agent	tcp.RtoMax	1.3.6.1.2.1.6.3.0	Text	1 Hour (3600)	90		No	
TCP Errors		TCP InErrs	SNMPV2 agent	tcp.InErrs	1.3.6.1.2.1.6.14.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
	TCP OutRsts	SNMPV2 agent	tcp.OutRsts	1.3.6.1.2.1.6.15.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	UDP InDatagrams	SNMPV2 agent	udp.InDatagrams	1.3.6.1.2.1.7.1.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	UDP NoPorts	SNMPV2 agent	udp.NoPorts	1.3.6.1.2.1.7.2.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	UDP InErrors	SNMPV2 agent	udp.InErrors	1.3.6.1.2.1.7.3.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	UDP OutDatagrams	SNMPV2 agent	udp.OutDatagrams	1.3.6.1.2.1.7.4.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP Packet Type Statistics	SNMP InPkts	SNMPV2 agent	snmp.InPkts	1.3.6.1.2.1.11.1.0	Numeric(Float)	1 Minute (60)	90	Pkts/s	No
		SNMP OutPkts	SNMPV2 agent	snmp.OutPkts	1.3.6.1.2.1.11.2.0	Numeric(Float)	1 Minute (60)	90	Pkts/s	No
		SNMP InTraps	SNMPV2 agent	snmp.InTraps	1.3.6.1.2.1.11.19.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		SNMP OutTraps	SNMPV2 agent	snmp.OutTraps	1.3.6.1.2.1.11.29.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		SNMP InTotalReQVars	SNMPV2 agent	snmp.InTotalReQVars	1.3.6.1.2.1.11.13.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
		SNMP InTotalResPVars	SNMPV2 agent	snmp.InTotalResPVars	1.3.6.1.2.1.11.14.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No
SNMP InSetReqs		SNMPV2 agent	snmp.InSetReqs	1.3.6.1.2.1.11.17.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
SNMP OutGetReqs		SNMPV2 agent	snmp.OutGetReqs	1.3.6.1.2.1.11.15.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
SNMP InGetReqs		SNMPV2 agent	snmp.InGetReqs	1.3.6.1.2.1.11.25.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
SNMP OutGetResPns		SNMPV2 agent	snmp.OutGetResPns	1.3.6.1.2.1.11.18.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
SNMP InGetResPns		SNMPV2 agent	snmp.InGetResPns	1.3.6.1.2.1.11.28.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
SNMP OutGetNexts		SNMPV2 agent	snmp.OutGetNexts	1.3.6.1.2.1.11.16.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
SNMP Errors	SNMP InErrAuthNxts	SNMPV2 agent	snmp.InErrAuthNxts	1.3.6.1.2.1.11.11.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP OutErrAuthNxts	SNMPV2 agent	snmp.OutErrAuthNxts	1.3.6.1.2.1.11.12.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InBadAuthNxts	SNMPV2 agent	snmp.InBadAuthNxts	1.3.6.1.2.1.11.30.0	Character	1 Hour (3600)	90	Link Up Down Trap Enable	No	
	SNMP InBadVersions	SNMPV2 agent	snmp.InBadVersions	1.3.6.1.2.1.11.3.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InBadCommunityNames	SNMPV2 agent	snmp.InBadCommunityNames	1.3.6.1.2.1.11.4.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InBadCommunityUses	SNMPV2 agent	snmp.InBadCommunityUses	1.3.6.1.2.1.11.5.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InASnmpParseErrs	SNMPV2 agent	snmp.InASnmpParseErrs	1.3.6.1.2.1.11.6.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InToolBgs	SNMPV2 agent	snmp.InToolBgs	1.3.6.1.2.1.11.8.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InNoSuchNames	SNMPV2 agent	snmp.InNoSuchNames	1.3.6.1.2.1.11.9.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InBadValues	SNMPV2 agent	snmp.InBadValues	1.3.6.1.2.1.11.10.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP InErrs	SNMPV2 agent	snmp.InErrs	1.3.6.1.2.1.11.20.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
	SNMP OutNoSuchNames	SNMPV2 agent	snmp.OutNoSuchNames	1.3.6.1.2.1.11.21.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No	
SNMP OutBadValues	SNMPV2 agent	snmp.OutBadValues	1.3.6.1.2.1.11.22.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No		
SNMP OutGenErrs	SNMPV2 agent	snmp.OutGenErrs	1.3.6.1.2.1.11.24.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No		
SNMP SilentDrops	SNMPV2 agent	snmp.SilentDrops	1.3.6.1.2.1.11.31.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No		
SNMP ProxyDrops	SNMPV2 agent	snmp.ProxyDrops	1.3.6.1.2.1.11.32.0	Numeric(Float)	1 Minute (60)	90	365 Delta (speed per second)	No		

Anexo X

Estudo completo da alarmística do
Access Point

SNMP Errors	SNMP InBadVersions	Yes IP RoutingDiscards	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(#2)>10) (Access Point:ip.HdrErrors.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(#2)>10) (Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10) (Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(#2)>10) (Access Point:ip.HdrErrors.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(#2)>10) (Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10) (Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(#2)>10) (Access Point:ip.HdrErrors.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(#2)>10) (Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many Routing Discards!	No	
	SNMP InBadCommunityNames	Yes IP In HdrErrors	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.HdrErrors.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In Header Errors!	No	
	SNMP InBadCommunityUses	Yes IP In AddrErrors	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In AddrErrors!	No	
	SNMP InASNParseErrs	Yes IP In UnknownProtos	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In Unknown Protos!	No	
	SNMP InTooBig	Yes IP RoutingDiscards	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many Routing Discards!	No	
	SNMP InNoSuchNames	Yes IP In HdrErrors	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.HdrErrors.last(,300)>10 & (Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In Header Errors!	No	
	SNMP InBadValues	Yes IP In AddrErrors	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In AddrErrors!	No	
	SNMP InGenErrs	Yes IP In UnknownProtos	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In Unknown Protos!	No	
	SNMP OutTooBig	Yes IP RoutingDiscards	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many Routing Discards!	No	
	SNMP OutNoSuchNames	Yes IP In HdrErrors	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.HdrErrors.last(,300)>10 & (Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In Header Errors!	No	
	SNMP OutBadValues	Yes IP RoutingDiscards	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(,300)>10 & (Access Point:ip.in.HdrErrors.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many Routing Discards!	No	
	SNMP OutGenErrs	Yes IP In HdrErrors	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.HdrErrors.last(,300)>10 & (Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In Header Errors!	No	
	SNMP SilentDrops	Yes IP In AddrErrors	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.InAddrErrors.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.in.UnknownProtos.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In AddrErrors!	No	
	SNMP ProxyDrops	Yes IP In UnknownProtos	+10 errors for 5 minutes (300)	Warning	((Access Point:ip.in.UnknownProtos.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(,300)>10 & (Access Point:ip.RoutingDiscards.last(#2)>10)	Access Point (HOSTNAME) It's reporting too many In Unknown Protos!	No	
	TCP Statistics	TCP InSegs	No					No
		TCP OutSegs	No					No
TCP ActiveOpens		No					No	
TCP PassiveOpens		No					No	
TCP AttemptFails		No					No	
TCP EstabResets		No					No	
TCP CurrEstab		No					No	
TCP RetransSegs		No					No	
TCP RTOAlgorithm		No					No	
TCP RstIn		No					No	
TCP	TCP RstOut	No					No	
	TCP InBacklog	No					No	
	TCP InMaxConn	No					No	
	TCP InErrs	No					No	
TCP Errors	TCP OutRsts	No					No	
	TCP InRsts	No					No	
UDP Statistics	UDP InDatagrams	No					No	
	UDP NoPorts	No					No	
	udpInErrors	No					No	
	udpOutDatagrams	No					No	

Graphs	Name	Necessary?	Trigger Name	Trigger Fire	Severity	Expression	Message	Depends	Check?
Interface	IF Number	No							No
	IF Name.Ra0	No							No
	IF Descr.Ra0	No							No
	IF Type.Ra0	No							No
	IF Speed.Ra0	No							No
	IF PhysAddress.Ra0	No							No
	IF AdminStatus.Ra0	No							No
	IF OperStatus.Ra0	No							No
	IF HighSpeed.Ra0	No							No
	IF Alias.Ra0	No							No
	IF CounterDiscontinuityTime.Ra0	No							No
	IF PromiscuousMode.Ra0	No							No
	IF LinkUpDownTrapEnable.Ra0	No							No
	IF ConnectorPresent.Ra0	No							No
IF LastChange.Ra0	No							No	
Non Unicast Packets	IF InMulticastPkts.Ra0	No							No
	IF InBroadcastPkts.Ra0	No							No
	IF OutMulticastPkts.Ra0	No							No
	IF OutBroadcastPkts.Ra0	No							No
	IF HClMulticastPkts.Fa0	No							No
	IF HClBroadcastPkts.Fa0	No							No
	IF HCOmulticastPkts.Fa0	No							No
	IF HCOBroadcastPkts.Fa0	No							No
IF InNUcastPkts.Ra0	No							No	
IF OutNUcastPkts.Ra0	No							No	
Unknown Protocols	IF InUnknownProtos.Ra0	No							No
	IF OutQLen.Ra0	No							No
Errors	IF InDiscards.Ra0	No							No
	IF InErrors.Ra0	No							No
	IF OutDiscards.Ra0	No							No
	IF OutErrors.Ra0	No							No
Traffic	IF InOctets.Ra0	No							No
	IF HClOctets.Ra0	No							No
	IF OutOctets.Ra0	No							No
	IF HCOctets.Ra0	No							No
	IF TotalInOctets.Ra0	No							No
IF TotalOutOctets.Ra0	No							No	
Unicast Packets	IF InUcastPkts.Ra0	No							No
	IF HClUcastPkts.Ra0	No							No
	IF OutUcastPkts.Ra0	No							No
	IF HCOUcastPkts.Ra0	No							No

Anexo XI

Processo de envio de notificações



IPO PORTO

INSTITUTO PORTUGUÊS DE ONCOLOGIA DO PORTO FG, EPE

Processo de envio de notificações



Carlos Miguel Porto de Almeida

Novembro 2014

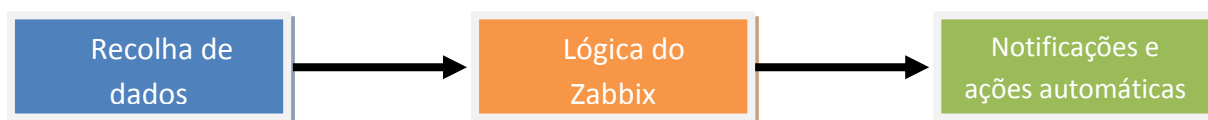
Visão geral

O funcionamento do sistema de notificações do Zabbix passa por três pontos-chave sequenciais que fazem com que as ações/notificações possam ser lançadas.

O primeiro ponto é a recolha de dados. Para que se possam receber notificações há que primeiro saber qual o equipamento, os itens relevantes e os tempos de monitorização. Estando estes elementos devidamente configurados é iniciada a recolha dos dados.

O segundo ponto é a configuração da lógica implementada no Zabbix. Isto de modo a que o Zabbix tenha forma de confrontar dos dados recolhidos com essa lógica de maneira a identificar a existência de problemas assim como o término dos mesmos.

O terceiro ponto é a reação a esses problemas onde o sistema de notificações entre em ação. Este sistema contém vários métodos de notificações e ações automáticas aos problemas.



Recolha de dados

O processo de recolha de dados envolve toda a fase de configuração do servidor/proxy do Zabbix. Devem ser tomadas em conta nesta fase todos os equipamentos que se deseja monitorizar, os seus itens e mais importante que tipo de recolha e que vai ser efetuada.

Essa escolha passa por uma recolha ativa passiva ou com a utilização de traps.

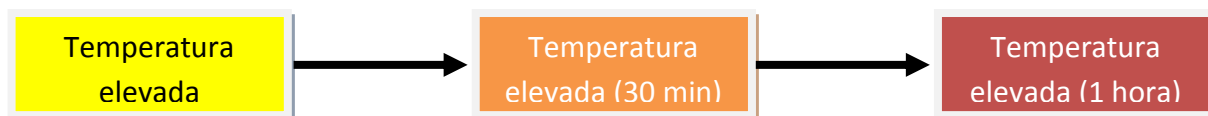
- Ativa – Este método é utilizado com o recurso de agentes instalados no equipamento. O agente inicia a comunicação e envia apenas os dados requeridos pelo servidor.
- Passiva – Este método é utilizado com o recurso a protocolos (SNMP, IPMI). O servidor inicia a comunicação e o equipamento envia os dados.
- Traps – Este método é utilizado com o recurso de agendamentos e eventos por parte do equipamento. Num intervalo de tempo definido ou no acontecimento de um evento o equipamento envia um conjunto de dados para o servidor.

Lógica do Zabbix

O processo de lógica do Zabbix envolve toda a fase de configuração das expressões que devem ser confrontadas com os dados recolhidos. Aqui devem ser definidas quais são os pontos críticos de alarme dos vários equipamentos e respetivos itens assim como a sua gravidade. A gravidade irá funcionar com um definidor de prioridades. Esta pode ser definida com vários níveis:

Gravidade	Prioridade	Tipos de problemas
Disaster	Muito alta	Falha de sistemas críticos
High	Alta	Falha de sistemas funcionais
Average	Media	Valores anormais do sistema
Warning	Baixa	Avisos do sistema
Information	Muito baixa	Informações do sistema
Not Classified	Variável	Outros casos

Estas expressões podem ser simples, como {espaço em disco <500MB}, ou complexas, como {(valor do processador > 70) & (número de processos < 1000)}. O Zabbix também permite a criação de dependências nos triggers. Esta funcionalidade permite que ao longo do tempo o problema possa escalar o seu nível de prioridade.



Estando os três problemas ligados entre si. O segundo só dispara se o 1 estiver ativo, e assim adiante. Cada nível de gravidade tem as suas próprias ações e métodos de notificação.

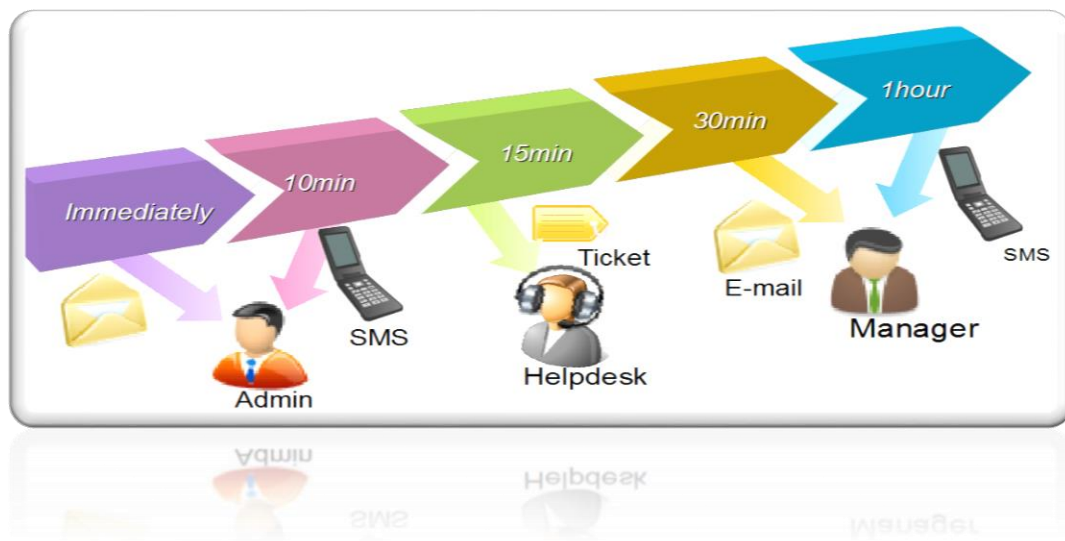
Notificações e ações automáticas

O processo de notificações e ações automáticas envolve toda a fase definição das ações a serem tomadas em tendo em conta o nível de gravidade. Essas ações passam por, ou pelo envio de uma notificação ou na execução de comandos remotos.

O Zabbix contém quatro meios de notificar os vários utilizadores:

- E-mail – Envio de correio eletrónico para um utilizador ou grupo de utilizadores.
- SMS – Envio mensagens para telemóvel de um utilizador ou grupo de utilizadores.
- Jabber- Envio de mensagens para o IM Jabber de um utilizador ou grupo de utilizadores.
- Script- Executar um script que vai iniciar uma outra forma de notificação ao ação automática.

As notificações podem ser intercaladas, escalonando-as por vários períodos de tempo e diferentes utilizadores.



Esta funcionalidade permite, na eventualidade de a primeira linha de resposta ao problema não atuar, a segunda linha possa ter conhecimento para que possa atuar. Também existe a funcionalidade que permite evitar que flutuações de problemas sejam constantemente reportadas, atrasando o processo de notificação num intervalo de tempo definido, onde só se o problema se mantiver contante durante esse tempo é que uma notificação é enviada.

Anexo XII

Nova arqutetura Zabbix



IPOPORTO

INSTITUTO PORTUGUÊS DE ONCOLOGIA DO PORTO FG, EPE

ESCALAR ZABBIX

ESTUDO DE ALTA DISPONIBILIDADE E PERFORMANCE

ZABBIX

Carlos Miguel Porto de Almeida

Junho 2014

ÍNDICE

Índice	125
Sistema atual	126
Arquitetura	128
Hardware	130
Alta disponibilidade do servidor	131
Alta disponibilidade da base de dados	132
Zabbix Proxies	133
Performance da base de dados	134
Receção de dados: passivo ou activo?	136
Monitorização do Servidor/Proxy	137
Elaboração de cópias de segurança	138

SISTEMA ATUAL

O sistema que se encontra em produção no momento está implementado de uma forma a permitir a monitorização de um conjunto de equipamentos importantes que garante o bom funcionamento de todos os serviços dentro da instituição.

Parameter	Value	Details
Zabbix server is running	Yes	127.0.0.1:10051
Number of hosts (monitored/not monitored/templates)	497	124 / 74 / 299
Number of items (monitored/disabled/not supported)	3061	1398 / 1188 / 274
Number of triggers (enabled/disabled) [problem/ok]	933	843 / 90 [17 / 826]
Number of users (online)	20	3
Required server performance, new values per second	20.61	-

Updated: 14:38:53

ILUSTRAÇÃO 1 - ESTADO PRESENTE DO SISTEMA

Como a quantidade de itens junto com os *triggers* a eles associados é baixa, este executa as suas tarefas de monitorização e alarmística sem problemas de maior relevância, sendo apresentado como uma solução bastante estável para o cenário atual.

Baseando-se numa arquitetura simples sendo composta por uma máquina única, onde está alojado o servidor de Zabbix versão 2.2.3, a sua base de dados e o *Webfront*, maquina essa que por seu lado se liga aos equipamentos de modo a receber a informação, podendo estes também se ligarem ao servidor para enviar informação.

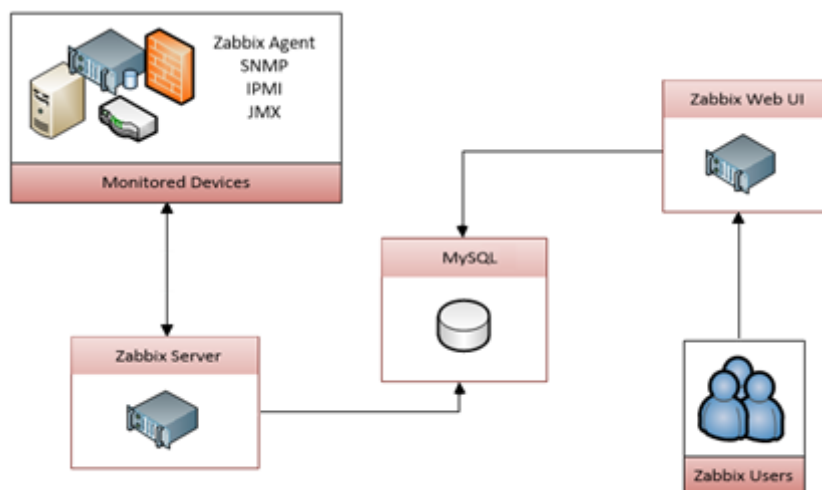


ILUSTRAÇÃO 2 - DIAGRAMA DA ARQUITETURA ATUAL

Esta arquitetura apesar de estável na configuração atual, ao incrementar o novo cenário ao já existente, observou-se que esta não se enquadra pois a carga de novos itens e *triggers* é demasiada para se manter estável. Devido a massiva

quantidade de novos dados, a sua leitura e escrita na base de dados faz com que haja um aumento de instabilidade o que leva o Zabbix começa a lançar falsos alarmes, até chegar ao ponto de bloquear e parar completamente. O I/O que a base de dados sofre com o aumento de dados cria um *bottleneck* crítico pois não tem poder de processamento. O facto de todos os elementos que consistem o sistema estarem na mesma máquina também é de relevância, fazendo com que processamento, alocação de memória e pesquisas sejam efetuadas pelo mesmo processador, disco e módulo de memória, levando assim a uma perda de performance do servidor.

Em baixo é possível observar a quantidade de novos valores que serão introduzidos ao introduzir todos os bastidores, access points e ups existentes na instituição que vão ser monitorizados. A estes valores tem que ser adicionados todos os já existentes.

TABELA 14 - QUANTIDADE DE NOVOS VALORES

Host			Items			Triggers		
Host	Type	Hosts	Items	Host/Type	Total/Type	Triggers	Host/Type	Total/Type
Switch	24	4	1814	4	7256	487	4	1948
Switch	24 - 24	1	3504	1	3504	960	1	960
Switch	24 - 50	1	5402	1	5402	1480	1	1480
Switch	48	15	3566	15	53490	967	15	14505
Switch	48-24	1	5256	1	5256	1440	1	1440
Switch	48-48	15	7008	15	105120	1920	15	28800
Switch	48 - 48 - 24	1	8760	1	8760	2400	1	2400
Switch	48 - 48 - 48	1	10512	1	10512	2880	1	2880
Switch	48 - 48 - 48 - 48	1	14016	1	14016	3840	1	3840
Switch	50	2	3712	2	7424	1007	2	2014
Switch	50 - 48	1	7154	1	7154	1960	1	1960
Switch	50 - 50	3	7362	3	22086	2007	3	6021
Partial Totals		46	78066	46	249980	21348	46	68248
Access Point	Cisco	13	186	13	2418	40	13	520
Partial Totals		13	186	13	2418	40	13	520
UPS	Riello	46	47	46	2162	27	46	1242
Partial Totals		46	47	46	2162	27	46	1242
Totals		105	78299	105	254560	21415	105	70010

Tendo estes fatores em vista, uma nova arquitetura terá que ser pensada e implementada de modo a permitir voltar a ter um sistema estável e também passível de ser escalável para novos elementos, pensando em futuras adições e aquisições.

ARQUITETURA

A nova arquitetura passa pela implementação de dois novos *clusters* assim como de um conjunto de *proxies*.

Os dois *clusters* vão estar vocacionados em dois pontos críticos no sistema:

- Base de dados MySQL - Esta tem que ter uma elevada disponibilidade, passível de aguentar com uma elevada carga de pedidos de leitura e escrita. É aconselhável a funcionar como ativo- ativo, e deve ter um armazenamento composto por 2 TB LUN replicados para outro igual como forma de disponibilidade, redundância e segurança.
- Servidor Zabbix – Esta componente é a que irá fazer a ponte entre as várias *proxies* criadas, donde irá receber a informação, analisa-la, despoletar os *triggers* e devidas ações e armazenar a informação recebida na base de dados. Deve também ter incorporado o Web UI que permitirá aos vários utilizadores a sua consulta de como o sistema se está a comportar, visualização de problemas e análise que permite redirecionar esforços para a raiz do problema e elaboração de relatórios.

A divisão da monitorização por várias *proxies*, permite dispersar a carga de recolha de dados do servidor Zabbix, pois são eles que a farão, armazenado numa base de dados local sendo depois esta enviada para o servidor em intervalos de tempo, permitindo ao servidor dar vazão a toda a informação. Na eventualidade de perda de comunicação entre as *proxies* e o servidor, este mantém essa informação durante um intervalo de tempo definido e na restituição das comunicações essa informação possa ser enviada para o servidor garantindo assim uma baixa ou quase nula perda de informação.

As *proxies* deverão ser divididas em três tipos de equipamentos, estando uma delas vocacionada a todos os servidores e bases de dados, outra para os aplicativos de rede e seus equipamentos de suporte e a terceira ficaria para a monitorização de media centers, quiosques e outras maquinas de elevado relevo.

A implementação de *proxies* permite uma escalabilidade ao sistema podendo ser criados novos e incorporados no sistema sem a necessidade de grandes configurações.

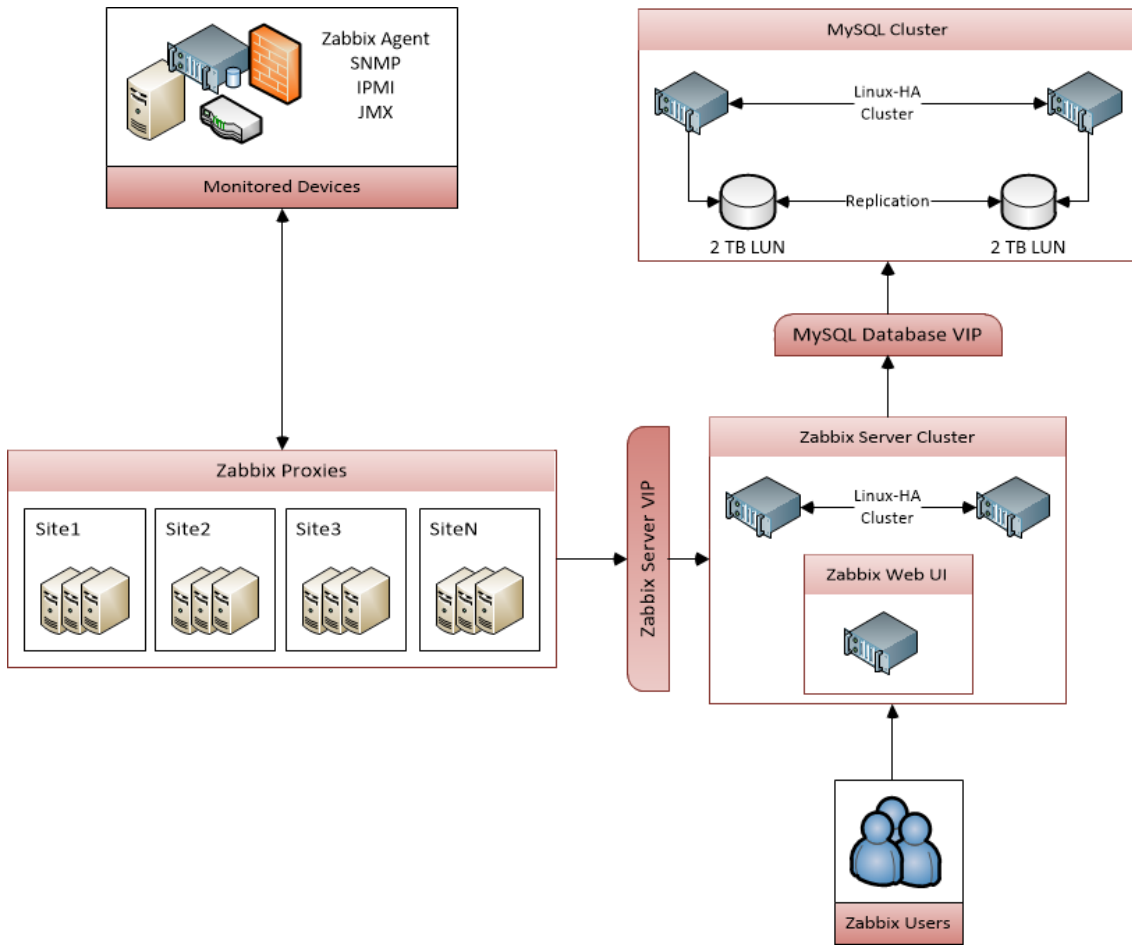


ILUSTRAÇÃO 3 - NOVA ARQUITETURA DO SISTEMA

HARDWARE

Aplicar a nova arquitetura implica que o hardware envolvido seja repensado e alterado consoante as novas necessidades. Devido a alta necessidade de leitura e escrita de pedidos na base de dados esta deve ser construída tendo como objetivo uma performance elevada. Para isso propõem-se a criação de um *cluster* com máquinas físicas a funcionar com ativo-ativo e com uma boa capacidade de armazenamento. Em teoria quanto mais rápidos os discos rígidos da base de dados, maior é a quantidade de dados que o Zabbix pode tratar. O CPU e memória também são importantes para a base de dados. Ao instalar uma boa quantidade de memória o Zabbix irá armazenar os dados com maior procura nela, o que leva a um incremento de performance, pois não tem fazer uma nova pesquisa ficando esta em cache. Propõem-se também a criação de um sistema de replicação em duas bases de dados garantindo assim um *backup* e uma maior segurança.

O servidor de Zabbix vai ser responsável pela avaliação de centenas de milhares de itens, *triggers* e gráficos. Isso requer que este tenha um poder de processamento elevado. Para obter esse efeito propõem-se a criação de um *cluster*, se possível físico, que seja capaz de tratar de todas as avaliações e alarmística. A questão de capacidade de armazenamento não se poem tanto aqui pois não e o seu propósito, quanto a memoria convém encontrar um valor sensato.

Na questão das *proxies* a melhor opção passa pela virtualização das máquinas visto que vão servir mais como colecionadores de dados a enviar para o servidor. O número de *proxies* a criar vai depender da divisão dos vários tipos de equipamentos, sendo a proposta inicial de três *proxies* (Servidores, Rede e Outros).

TABELA 2 PROPOSTA DE HARDWARE E SOFTWARE

Zabbix server	Zabbix database	Zabbix proxies	SAN
12x cores 4GB memory 128GB disk CentOS 6.5 x64 Zabbix 2.2.4	12x cores 8GB memory 2TB SAN CentOS 6.5 x64 MySQL 5.6.12+	4x cores 2GB memory 50GB disk CentOS 6.5 x64 Zabbix 2.2.4 MySQL 5.6.12+	2x 2TB LUN

ALTA DISPONIBILIDADE DO SERVIDOR

Como não é possível ter duas instancias do servidor Zabbix a correr em simultâneo assim como também não é tolerável ter longo períodos de *downtime* no serviço de monitorização, propõem-se a criação de um cluster Linux-HA utilizando Pacemaker e CMAN ([exemplo de configuração](#)), assegurando assim a confiabilidade, disponibilidade e facilidade de manutenção.

Em baixo segue uma lista de serviços suportados pela tecnologia HA que deverão ser configurados:

- Partilha de endereço IP
 - No evento de falha do servidor (*Failover*) o IP deverá ser dissociado do servidor em falha e ser atribuído ao servidor recém-ativo.
 - Esse IP será sempre associado ao servidor ativo, o que traz três benefícios para o sistema:
 - Facilidade em encontrar o servidor ativo;
 - Todas as conexões do servidor Zabbix ativo vêm do mesmo IP bastando para isso configurar a entrada “SourceIP” no ficheiro de configuração (`zabbix_server.conf`);
 - Todas as *proxies* e agentes podem ser configurados para apontar para o endereço de IP partilhado para chegar ao servidor Zabbix ativo.
- Processo “zabbix_server”
 - No evento de falha do servidor (*Failover*) o processo “zabbix_server” deverá ser interrompido no servidor em falha e ser iniciado no servidor recém-ativo.
- Um *symlink* para *crons*
 - Este aponta para um diretório que contem todos os *crons* e que só devem ser executados no servidor ativo. O *crontab* de cada servidor deve aceder a todos os *crons* através deste *symlink*.
 - No evento de falha do servidor (*Failover*) o *symlink* deverá ser excluído no servidor em falha e ser criado no servidor recém-ativo.
- Processo *cron* (*crond*)
 - No evento de falha do servidor (*Failover*) o *crond daemon* deverá ser interrompido no servidor em falha e ser iniciado no servidor recém-ativo.

ALTA DISPONIBILIDADE DA BASE DE DADOS

A base de dados é um dos componentes importantes do sistema, que deve ser projetada de modo a garantir um funcionamento contínuo, resistente a falhas, e permitir um sistema de replicação/*backup*. A base de dados também deverá ser composta por um *cluster* Linux-HA utilizando Pacemaker e CMAN ([exemplo de configuração](#)) pois permite um bom desempenho no controlo da replicação MySQL. Essa replicação permite manter uma sincronização entre o servidor ativo e passivo de MySQL, sendo necessário a configuração dos seguintes serviços:

- Partilha de endereço IP
 - No evento de falha do servidor (Failover) o IP deverá ser dissociado do servidor em falha e ser atribuído ao servidor recém-ativo.
 - Esse IP será sempre associado ao servidor ativo, o que traz dois benefícios para o sistema:
 - Facilidade em encontrar o servidor ativo;
 - No evento de falha do servidor (Failover), não é necessário efetuar qualquer alteração no servidor de Zabbix para apontar a nova base de dados ativa.
- Partilha de endereço IP secundário
 - Este IP deve ser utilizado apenas quando o acesso a base de dados do Zabbix é de leitura. Desta forma pedidos do tipo *ad-hoc* podem ser efetuados a base de dados passiva em vez de a ativa.
 - Este IP pode estar em ambos os servidores, ativo e passivo. Essa decisão depende das condições:
 - Se o servidor passivo estiver *online* e o MySQL não tiver um atraso, em relação ao ativo, inferior a sessenta segundos, este IP vai para o servidor passivo;
 - Se o servidor passivo estiver *offline* ou com um atraso, em relação ao ativo, superior a sessenta segundos, este IP vai para o servidor ativo.
- Processo “mysqld”
 - No evento de falha do servidor (*Failover*) a instancia do servidor recém-ativo torna-se o MySQL principal. Quando o novo servidor recém-passivo ficar disponível, este torna-se um secundário do novo principal.

ZABBIX PROXIES

A utilização de *proxies* permite que se possa dividir a monitorização por múltiplas máquinas, não centralizando tudo no servidor Zabbix, o que leva a que a carga do processador seja atenuada, ganhando performance. As *proxies* são responsáveis por enviar toda a informação que recolheram para o servidor de Zabbix a analisar.

Ao configurar as *proxies* de Zabbix existem alguns pontos a tomar em consideração:

- Conseguem lidar com uma quantidade incrível de dados de entrada;
- Configuradas corretamente permitem monitorizar entre mil e quinhentos a mil setecentos e cinquenta NVPS sem problemas;
- Não é necessário grandes máquinas a nível de hardware, uma VM com 2vCPU, 4GB RAM e uma base de dados local são suficientes;
- No caso de a conexão entre a *proxy* e o servidor for quebrada, esta guarda a informação recolhida na base de dados local e quando a conexão for reposta essa informação é enviada. Nunca há perda de informação.
- A latência da rede é um fator importante a ter em conta, pois os funcionamento das *proxies* passam por:
 - A *proxy* inicia uma ligação ao servidor;
 - Envia até um máximo de mil valores;
 - Fecha a ligação.
- Este passos são efetuados quantas vezes forem precisa, mas se os valores da latência não formem tomadas em conta este processo torna-se lento, devido especialmente a duas questões principais:
 - A conexão inicial é lenta;
 - Uma vez que a ligação é fechada após o envio de mil valores, a conexão TCP não existe em tempo suficiente de modo que possa acelerar a largura de banda disponível no canal.

PERFORMANCE DA BASE DE DADOS

A base de dados é um ponto pontos críticos para formular uma solução escalável de Zabbix. Como a carga de escrita na base de dados é massiva, a performance de I/O esta diretamente ligada a *bottlenecks* sendo este um dos problemas mais fáceis de se encontrar, onde a sua solução necessita de estudo na configuração da mesma.

De marcar que o “Com_update” têm o maior número de pedidos por segundo. Isto acontece porque todos os valores recebidos pelo Zabbix resultam de atualizações à tabela de itens da base de dados. Outro ponto a marcar é que a base de dados é *write-heavy*, isto significa que a *cache* das *queries* MySQL não ajuda a performance, muito pelo contrário causa uma perda de performance devido a constante necessidade de marcar as *stores queries* como invalida a medida que esta são atualizadas.

O “Zabbix Housekeeping” também é um destruidor de performance da base de dados, em grandes ambientes de monitorização, pelo qual é recomendado desabilita-lo. Ao desabilitar esta funcionalidade toda a informação relativa a histórico/eventos/ações deixa de ser apagada automaticamente. Uma solução para contornar esta limitação é particionar as tabelas da base de dados. Infelizmente essa solução não funciona com tabelas que utilizem chaves estrangeiras, o que não é o caso das tabelas de histórico. Particionar as tabelas de histórico produz dois benefícios:

- Toda a informação existente numa tabela de um determinado dia/semana/mês pode ser contida dentro da sua própria partição. Isso permite uma fácil eliminação dos dados antigos, com pouco ou mesmo nenhum impacto no servidor da base de dados e torna também mais fácil de perceber quanta informação é “puxada” para o sistema no período de tempo que foi determinado na partição.
- Ao utilizar tabelas MySQL *InnoDB* a ação de apagar dados das tabelas não liberta espaço em disco, simplesmente são criadas áreas nos *namespace InnoDB* que podem, mais tarde, guardar novos dados. É impossível encolher os *namespace InnoDB*, no entanto as partições podem ser apagadas, libertando assim espaço em disco.

Habilitar a funcionalidade de “Large Pages”(exemplo de configuração), quando a arquitetura assim o permite, trás também um incremento de performance da base de dados.

A utilização de um *filesystem* *tmpfs* para ficheiros temporários permite que, ao utilizar a memória em vez dos discos locais, a criação de tabelas temporárias no MySQL seja efetuada muito mais rapidamente (exemplo de configuração). Esta medida melhora a performance e diminui a carga do servidor pois não cria filas de espera e *bottlenecks* nos discos rígidos.

A nível de performance a opção mais importante, que deve ser devidamente configurada, é a Innodb Buffer Pool. Utilizando um servidor dedicado onde apenas se utiliza tabelas Innodb, como é proposto nesta nova arquitetura, deve-se ponderar a atribuição de toda a memória, que não seja utilizada, a Innodb Buffer Pool. Esta deverá ter um valor por volta de 10% superior a informação armazenada (espaço total da Innodb TableSpaces), pois esta não contém apenas páginas de informação, contém também hash indexes adaptativos, buffer de inserção, e de possíveis locks que também ocupam espaço. Innodb aloca mais memória em estruturas relacionadas com o buffer pool que aquela que é especificada. Por exemplo se alocar-nos 12GB para o buffer pool a total de memória alocada pelo Innodb é um pouco superior a 13GB.

Depois de decidir qual o tamanho da base de dados é necessário analisar se existem restrições a Innodb Buffer Size as quais se podem recorrer. Este passo aplica-se em sistemas de 32bit em ambientes Windows. Estas restrições são normalmente aplicadas quanto ao total de memória que os processos podem alocar, onde convém garantir que existe espaço em memória para que as outras necessidades do MySQL possam ser cumpridas.

Outro passo importante é analisar e definir a quantidade de memória que é necessária de modo a que as necessidades do sistema possam ser cumpridas fazendo com que este execute a sua tarefa em plena capacidade.

RECEÇÃO DE DADOS: PASSIVO OU ACTIVO?

O Zabbix proporciona dois métodos diferentes de recepção de dados: ativo ou passivo. O servidor/*proxies* de Zabbix “puxam” dados dos agentes para os itens passivos e os agentes “empurram” os dados para o servidor/*proxies* Zabbix para os itens ativos. A escolha do tipo de monitorização usado vai ter um efeito drástico sobre quantidade de informação capaz de processar com sucesso.

- Monitorização passiva requer processos de “polling” por parte do servidor/*proxies*, efetuando um pedido de informação a um agente ficando depois a espera de uma resposta. Dependendo da rede e da performance dos equipamentos que estão a ser monitorizados o “poller” pode ter que estar a espera alguns segundos da resposta. multiplicando esse processo por dezenas ou centenas de equipamentos, pode transformar-se um processo lento.
- Monitorização ativa o servidor/*proxies* Zabbix fica a espera de uma conexão iniciada no agente. Cada agente individual liga-se periodicamente ao servidor/*proxies* de modo a obter uma lista de todos os itens que deve monitorizar, onde irá então recolher a informação dos itens, consoante o intervalo de tempo neles definidos, e envia-la para o servidor/*proxies* quando esta for necessária. Uma conexão só será estabelecida com o servidor/*proxies* quando tiver dados para enviar. Este método de monitorização evita que o servidor/*proxies* esteja a espera da resposta dos agentes, melhorando assim a velocidade de recepção dos dados.

MONITORIZAÇÃO DO SERVIDOR/PROXY

Deve-se sempre monitorizar os processos internos do servidor Zabbix para se poder ter a noção de onde é que possíveis *bottlenecks* podem ocorrer assim como identificar processos que podem ser reduzidos, permitindo assim poupar recursos. A partir da versão 2.0.x o Zabbix já vem configurado com alguns itens de monitorização interna, itens esses que devem ser adicionados ao servidor!

Um dos itens que pode indicar problemas na base de dados é o espaço em disco livre na “*History Write Cache*” (variável que se encontra no ficheiro “conf” do servidor). Os valores deste item devem estar sempre perto dos 100%. Se a cache fica continuamente cheia, isso significa que o Zabbix não tem capacidade para acompanhar a escrita na base de dados com a entrada de novos dados.

Infelizmente as *proxies* não suportam estes itens, fazendo com que seja mais difícil identificar qual os problemas.

Outra questão com as *proxies* é que não existe uma maneira pré-configurada de saber quantos valores, do lado das proxies, faltam sincronizar no servidor. Felizmente existe uma maneira de dar a volta a essa questão permitindo assim saber o quanto a *proxy* esta atrasada. Para isso base criar uma *query* a base de dados da *proxy* do tipo:

```
SELECT ((SELECT MAX(proxy_history.id) FROM proxy_history)-nextid)
FROM ids WHERE field_name='history_lastid'
```

Adicionando depois um comando, no ficheiro de configuração do agente da *proxy*, do tipo “UserParameter” que deve ser adaptado consoante a base de dados da *proxy*. Este exemplo aplica-se a uma base de dados SQLite3:

```
UserParameter=zabbix.proxy.items.sync.remaining,/usr/bin/sqlite3
/path/to/the/sqlite/database "SELECT ((SELECT MAX(proxy_history.id)
FROM proxy_history)-nextid) FROM ids WHERE field_name='history_lastid'"
2>&1
```

Esta *query* vai retornar o número de valores que proxy ainda tem para enviar para o servidor.

No servidor cria-se um *trigger* que será despoletado se as *proxies* começarem a ficar congestionadas:

```
{Hostname:zabbix.proxy.items.sync.remaining.min(10m)}>100000
```

ELABORAÇÃO DE CÓPIAS DE SEGURANÇA

O sistema baseia-se na recolha e análise de informação de equipamentos. De modo a garantir que essa informação se encontra protegida deve-se pensar em criar sistemas e políticas de backup.

Ora como o IPO já possui políticas de cópias de segurança em tapes magnéticas, propôs-se que as mesmas sejam implementadas no novo sistema, separando as configurações dos dados recolhidos.

Como as configurações do sistema não são alteradas com grandes intervalos de tempo estas devem seguir a política de backup incremental, diario.

A informação recolhida como é de constante mudança terá que respeitar uma política de backup diario em regime de Full.

Anexo XIII

Plano para desenvolvimento futuro



IPO PORTO
INSTITUTO PORTUGUÊS DE ONCOLOGIA DO PORTO FG, EPE

Plano para desenvolvimento futuro



Carlos Miguel Porto de Almeida

Novembro 2014

Durante o período de duração do meu estágio no serviço de Informática fui analisando algumas questões que penso podem trazer uma melhoria não só ao serviço a nível funcional como também a nível de imagem do serviço na instituição.

Em baixo enumero um conjunto de pontos/ideias que penso poder executar e implementar de modo a que se possa atingir os objetivos acima referidos. Estes pontos/ideias irão permitir um melhor controlo e conhecimento do estado de todo o parque informático, podendo assim decrementar o tempo perdido na procura de problemas, partindo diretamente para a resolução, procura das causas e mitigação das mesmas. A tentativa de redução dos incidentes reportados a informática tem também um papel importante pois demonstra ao utilizador final que a informática trabalha e tenta efetuar sempre o melhor serviço.

Os pontos que considero passíveis de análise são:

- Levantamento de requisitos onde tem que ser analisado todos os itens referentes a todo o equipamento que se deseja monitorizar, envolvendo todos os elementos da equipa do serviço de informática. Este trabalho já se encontra em desenvolvimento e requer, por parte dos elementos da equipa, uma análise e feedback de modo a que se possa estabelecer um sistema robusto, fiável, confiável e ao mesmo tempo escalável.
- Instalação da nova infraestrutura de Zabbix, (criação de dois clusters, um de base de dados e outro do servidor Zabbix, e das várias proxies a introduzir).
- Configuração e otimização de todos os elementos da nova infraestrutura (Bases de dados, Servidores e proxies), para que o sistema corra sem problemas de acesso a informação e fornecendo informação correta e fiável.
- Estudo, limpeza e reestruturação da monitorização/alarmística já implementada, pois foram detetados certos itens que estão duplicados, em contradição, não suportados pelos equipamentos e alguns inúteis.
- Migração do sistema atual para a nova infraestrutura para que todo trabalho já efetuado até a data não se perca.
- Estudo e implementação de novos itens de monitorização, e respetiva alarmística, seguindo interesse mostrado por vários elementos da equipa de informática:
 - Quiosques -> Perda de ligação com o servidor;
 - Quiosques -> Bloqueio de spool das impressoras;
 - Internet -> Falha do serviço de internet;
 - Hardware -> Verificação de discos (Espaço livre/ocupado);
 - Servidores -> Verificações de servidores de Windows e Linux;
 - Serviços -> Estado de Biztalk, Exchange;
 - Bases de dados -> Estado de todas as bases de dados;
 - Servidores Web -> Estado do Apache, Tomcat e IIS;
 - BackUps -> Informação de falha ao efetuar backups de serviços críticos;
- Ligar o Zabbix ao OTRS para que este, na existência de um problema, automaticamente crie um novo *ticket* para a (s) pessoa (s) devida (s).

- Implementação de escalabilidade das notificações, ou seja o problema deve ser direcionado para a pessoa correta e na eventualidade de impedimento dessa pessoa este, com o passar do tempo, posso ser encaminhado para outra pessoa e por ai adiante até o problema se encontrar resolvido. Esta funcionalidade permite que a resolução seja focada apenas nos intervenientes corretos. Esta ação pode ser definida para que no decorrer do tempo possam ser utilizados diferentes meios de notificação.
- Novo sistema de envio de mensagens de SMS (envio pela rede) em vez do atual (Script/Telemóvel). A implementação de um sistema mais fiável do que o existente na atual configuração. Estudo na aquisição de um equipamento que permita cortar custos com o envio de SMS e ao mesmo tempo garantido um serviço sem falhas e sempre disponível.
- Estudar a possibilidade de ligação do Zabbix ao sistema do sinfNotifica na inevitabilidade de “crash” ou sistemas em baixo os utilizadores seja notificado de um “downtime” do serviço evitando assim um contacto telefónico ou de outro tipo.
- Criação de uma página no portal onde será possível ver o estado dos vários servidores/serviços da instituição permitindo assim que o utilizador final a consulte previamente antes de efetuar o contacto com a informática.
- Estudo de possibilidade de ligação com a central telefónica para recolha de dados sobre tempos de espera médios, número de chamadas de entrada e atendidas, entre outros elementos.
- Elaboração de relatórios seguindo as normas ISO 9001 “*Quality Management Systems*” e/ou outras normas.
- Elaboração de trabalho de conversão dos dados de baixo nível da monitorização e aproveitá-los para gerar indicadores de alto nível para a organização através de um sistema de BI de auditoria.
- Apoio à instalação e configuração da nova infraestrutura de rede planeada pela instituição assim como da atual.
- Disponibilidade total para embarcar em outros projetos estando sempre aberto a novos desafios e horizontes.

O estudo, instalação, configuração, implementação destes vários projetos estão discriminados no mapa de Gant que disponibilizo em baixo de modo a poder ter uma ideia do tempo necessário para execução das tarefas.

Mapa de Gant

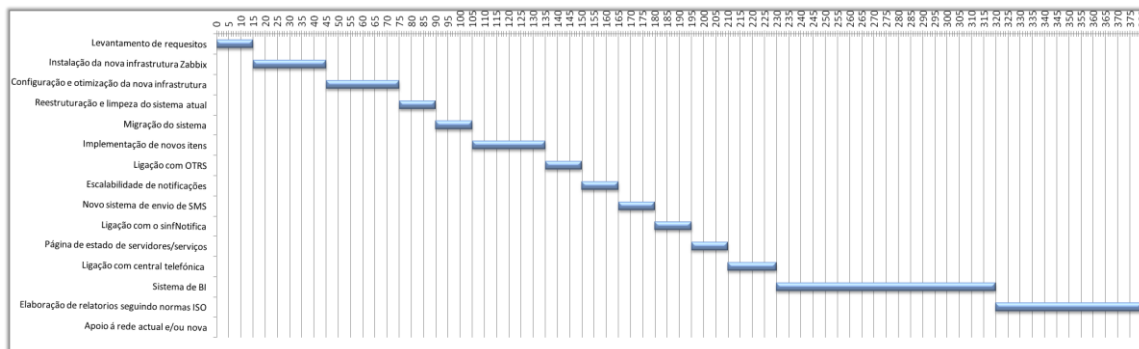


Ilustração 1 - Mapa de Gant apresenta tempo estimado por tarefa a realizar

Tarefa	Início	Duração (Dias)
Levantamento de requisitos	0	15
Instalação da nova infraestrutura Zabbix	15	30
Configuração e otimização da nova infraestrutura	45	30
Reestruturação e limpeza do sistema atual	75	15
Migração do sistema	90	15
Implementação de novos itens	105	30
Ligação com OTRS	135	15
Escalabilidade de notificações	150	15
Novo sistema de envio de SMS	165	15
Ligação com o sinfNotifica	180	15
Página de estado de servidores/serviços	195	15
Ligação com central telefónica	210	20
Sistema de BI	230	90
Elaboração de relatórios seguindo normas ISO	320	60
Apoio á rede actual e/ou nova	380	-
Total		365

Ilustração 4 – Tempo por tarefa