DM

Monitorização Distribuída de uma Instituição Governamental

DISSERTAÇÃO DE MESTRADO

Lisandro Henrique Gouveia de Olim Marote
MESTRADO EM ENGENHARIA INFORMÁTICA

UNIVERSIDADE da MADEIRA
A Nossa Universidade
www.uma.pt

setembro | 2024

Monitorização Distribuída de uma Instituição Governamental

DISSERTAÇÃO DE MESTRADO

Lisandro Henrique Gouveia de Olim Marote
MESTRADO EM ENGENHARIA INFORMÁTICA

ORIENTAÇÃO
Eduardo Miguel Dias Marques

COORIENTAÇÃO
Duarte da Silva Correia

Resumo

Este projeto de Mestrado em Engenharia Informática, visa a análise e implementação de uma monitorização distribuída numa instituição Governamental, de envergadura considerável, com especificidades e características próprias. A monitorização de rede e serviços de grande dimensão, além da escala, apresenta desafios de como organizar os dados monitorizados de forma eficiente e eficaz. A obtenção de dados de equipamentos e serviços remotos apresentam, por vezes, flutuações grandes, dependendo das redes de interligação. Outro problema, é a necessidade de servidores centrais de grande capacidade para a monitorização e processamento de todas as métricas de monitorização. Uma abordagem diferente a esta forma de monitorização, é a utilização de vários equipamentos de monitorização, nas tarefas de agregação de dados e de processamento de informação. É sempre necessário, à luz de cada cenário, organizar essa estrutura de monitorização da forma mais adequada e eficiente.

Palavras-Chave: Monitorização de Redes Distribuídas, Gestão de Sistemas e Redes, Alarmística, Instituição Governamental, Métricas de Monitorização, *Zabbix*.

Abstract

This project for the Master's Degree in Informatics Engineering aims to analyze and implement distributed monitoring in a government institution of considerable size, with its own specificities and characteristics. Monitoring large networks and services, in addition to their scale, present challenges in terms of how to organize the monitored data efficiently and effectively. Obtaining data from remote equipment and services sometimes present large fluctuations, depending on the interconnection networks. The need for large central servers to monitor and process all the sensors is another problem. A different approach to this form of monitoring is to use several monitoring devices and the tasks of data aggregation and processing. It is always necessary, in the light of each scenario, to organize this monitoring structure in the most appropriate and efficient way.

Keywords: Distributed Network Monitoring, System and Network Administrator, Alarm, Government Institution, Metrics for Monitoring, Zabbix.

Agradecimentos

Aproveito a oportunidade de poder agradecer e dar uma palavra de apreço a todos os que, duma forma ou de outra, contribuíram e suportaram a evolução de toda esta dissertação.

Quero agradecer especialmente ao orientador Eduardo Miguel Dias Marques, pela confiança depositada e oportunidade para realização de uma dissertação desta natureza, pelos esclarecimentos de dúvidas sempre oportunos, suas direções e observações com a sua experiência profissional e pessoal. Agradecer especialmente nos momentos menos bons, pelo seu espírito de liderança e de incentivo, por nunca ter desistido e ter sido e ser, um segundo pai ao longo não só neste projeto, mas ao longo destes anos.

Agradeço a cooperação da instituição Governamental, em especial ao Engenheiro Duarte da Silva Correia pela sua disponibilidade e suporte. Agradeço a partilha da sua experiência profissional, conselhos pessoais fundamentais no crescimento profissional e pessoal, tendo sido imprescindível ao longo das várias etapas do projeto.

Também quero agradecer aos meus colegas de trabalho em especial à Engenheira Manuela Pão, pela sua disponibilidade em demostrar o seu conhecimento como gestor de redes, tendo sido também fundamental na recolha de informação para posterior análise no projeto. Um especial agradecimento a todos os docentes da Universidade da Madeira na área das redes, desde o Professor Filipe Freitas o Engenheiro Marcos à Professora Lina Brito pela forma como transmitiu conhecimentos ao longo das suas aulas e cadeiras, forma essa que fez surgir um especial apreço pela área de gestão de sistemas e redes.

A todos estes que direta ou indiretamente contribuíram para a concretização deste projeto o meu Muito Obrigado!

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

AJAX	*Asyncronous JavaScript And XML*
API	*Application Programing Interface*
FCEE	*Faculdade de Ciências Exatas e da Engenharia*
CEE	*Ciências Exatas e da Engenharia*
CPE	*Customer Premises Equipment*
CPU	*Central Processing Unit*
CVE	*Common Vulnerabilities and Exposures*
DDNS	*Dynamic DNS*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
FCAPS	*Fault Configuration Accounting Performance Security*
GUI	*Graphical User Interface*
HTTP	*HyperText Transfer Protocol*
HTTPS	*HTTP Secure*
ICMP	*Internet Control Message Protocol*
IMPI	*Intelligent Platform Management Interface*
ISO	*Intertional Organization for Standardization*
ISP	*Internet Service Provider*
IT	*Information Technology*
JSON	*JavaScript Object Notation*
LDAP	*Lightweight Directory Access Protocol*
LTS	*Long Term Support*
MIB	*Management Information Base*
NAT	*Network Address Translation*
OID	*Object IDentifier*
PHP	*PHP: Hypertext Preprocessor*
QoS	*Quality of Service*
RMON	*Remote Network MONitoring*
SD-WAN	*Software-Defined Wide Area Network*
SMS	*Short Message Service*
SMPT	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*

SSH	*Secure SHell*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TMN	*Telecommunications Management Network*
UDP	*User Datagram Protocol*
UI	*User Interface*
UPS	*Uninterruptible Power Supply*
VM	*Virtual Machine*
XML	*eXtensible Markup Language*

1. Introdução

Com o crescimento de novos utilizadores e aumento das suas necessidades a nível de serviços, a área de gestão de sistemas e redes tem vindo a mostrar-se cada vez mais fundamental na gestão desta nova exigência, que os novos utilizadores vão impondo cada vez mais nas áreas das tecnologias da informação (TI) [1]. O desenvolvimento das redes foi acompanhando a exigência dos seus utilizadores e serviços, fazendo com que estes possuam mecanismos mais robustos e fiáveis, mas também mais complexos. Cuando existe uma falha na rede, determinados serviços deixam de estar disponíveis aos seus clientes. Este tipo de falhas implica custos e redução de produtividade, e, é nestas situações, que a monitorização dos vários serviços duma rede é necessário [2]. Devido a esta complexidade acrescida, a gestão de sistemas e redes teve a necessidade de garantir que seus sistemas estariam operacionais, garantindo aos seus clientes uma utilização fluente e fiável através de mecanismos de monitorização. Sistemas de monitorização mais convencionais possuem uma grande limitação, muitas das vezes transmitindo apenas informação sobre se o equipamento estará ligado ou não, informações essas que não são muito úteis para um administrador de sistemas e redes [3]. A monitorização de uma rede necessita duma alarmística e previsibilidade robusta, a qual auxilie o administrador de rede a detetar problemas que possam surgir, antes que estes de facto aconteçam.

A instituição Governamental onde este trabalho foi realizado possui, de forma dispersa, uma monitorização primitiva dos seus mais variados serviços como, secretarias, escolas, *datacenters*, entre outros. Atendendo às suas características próprias, pretende desenvolver uma monitorização distribuída, que colmate as suas necessidades particulares da própria instituição.

A solução eleita deve comportar-se como uma plataforma de gestão fortemente escalável, robusta e o mais completa possível dentro de um conjunto de soluções bem definidos. O desenvolvimento de componentes adicionais, visa cobrir alguns aspetos específicos da rede própria da instituição Governamental. Terá de estar preparada para situações de ocorrências previstas e fortemente escaláveis, dentro de processos bem definidos, debatidos ao longo de reuniões com Engenheiro Duarte da Silva Correia e com Professor Eduardo Miguel Dias Marques.

Este capítulo descreve o Projeto de Mestrado em Engenharia Informática, o propósito e âmbito do projeto desenvolvido. Enumera os objetivos delineados para médio e longo prazo, e apresenta a metodologia de trabalho adotada a cumprir com instituição Governamental. Sintetiza os capítulos e a distribuição respetiva ao longo do documento.

1.1. Contexto

Este projeto de Mestrado em Engenharia Informática assenta na área da gestão de sistemas e redes, mais concretamente na monitorização distribuída de sistemas. Serão descritas as plataformas de gestão e monitorização como solução integrada, como resposta às necessidades dos gestores de rede na monitorização de uma infraestrutura distribuída.

1.2. Objetivos

Os objetivos inicialmente definidos visam a instalação de uma plataforma para monitorização de uma rede distribuída. É pretendido a definição de processos que levam à configuração da monitorização de *datacenters* e serviços de rede, como também dos processos de manutenção e definição de elementos a monitorizar.

O objetivo principal é, efetivamente, focar-se na monitorização distribuída completa de *datacenters* e aprimorar todo o processo de gestão de redes com a monitorização e alarmística necessárias. Isto implicará pesquisar, analisar e comparar plataformas de gestão vigentes e selecionar a plataforma que melhor se enquadra no cenário descrito.

1.3. Metodologia

A metodologia adotada para o presente projeto de Mestrado foi composta por 4 etapas:

1. Recolher e estudar dados da infraestrutura da instituição Governamental, tendo por base a documentação facultada e respetivas reuniões com o Engenheiro Duarte da Silva Correia.

2. Pesquisar e analisar plataformas que melhor se enquadram tendo em conta as características e exigências da infraestrutura de rede e serviços da instituição Governamental.

3. Implementar a solução de gestão integrada, com componentes desenvolvidos para colmatar as lacunas identificadas.

4. Testar a solução implementada e reajustar parâmetros e/ou procedimentos de acordo com os resultados obtidos.

1.4. Organização

O presente documento encontra-se perfazendo num total de 7 capítulos, incluindo o capítulo atual, organizado da seguinte forma:

Capítulo 1: Introdução – contextualização do problema, onde é apresentado os objetivos delineados, como também a metodologia adotada para conclusão do Projeto de Mestrado em Engenharia Informática.

Capítulo 2: Estado da Arte – apresentação teórica de modelos, arquiteturas e conceitos de gestão e monitorização de redes.

Capítulo 3: Análise da Rede Institucional – descrição da infraestrutura de rede e serviços da instituição Governamental, e análise dos sistemas de monitorização existentes. Análise das lacunas identificadas e elaboração de requisitos.

Capítulo 4: Proposta Arquitetural – apresentação da proposta de arquitetura, como solução de monitorização para a instituição Governamental, tendo por base os requisitos elaborados e respetiva análise da rede institucional.

Capítulo 5: Implementação – configuração da solução aplicada ao cenário da infraestrutura e serviços da Instituição Governamental, assim como abordagem realizada ao problema de gestão existente.

Capítulo 6: Análise e Resultados – reflexão sobre a arquitetura e métodos vigentes na monitorização da instituição Governamental. Minuciar se os problemas inicialmente identificados estão ultrapassados e o seu porquê.

Capítulo 7: Conclusão – retrospetiva geral do trabalho efetuado, salientando direções a tomar para trabalho futuro.

2. Estado da Arte

As redes informáticas norteiam cada vez mais o sucesso empresarial, independentemente da dimensão do negócio e da complexidade da infraestrutura que as suportam [4]. Quando uma infraestrutura de rede falha, organizações e clientes por ela abrangidos deixam de poder comunicar. Esta situação implica custos e redução de produtividade, e é nestas situações que uma monitorização se torna necessário [5].

Nas últimas duas décadas, verificou-se um aumento da utilização da *internet,* do uso de aplicações que utilizam esta infraestrutura e, mais recentemente, a utilização de serviços na própria *internet* (*Cloud Computing*), conduzindo à necessidade de implementação de arquiteturas e sistemas de monitorização [6] [7].

Toda esta multiplicidade trouxe a necessidade de impor normas universais definidas através de modelos de referência, como é o caso do modelo *Open Systems Interconnection* (*OSI*) [8]. Estes modelos especificam como é efetuada a comunicação entre dispositivos, e descrevem os mecanismos usados na troca de informação [9]. Arquiteturas de monitorização distribuídas são conhecidas por serem desafiadoras na análise de dados em tempo real, especialmente quando o número de itens a monitorizar aumenta [10].

A gestão de redes é uma área fundamental, a qual garante um bom funcionamento de uma infraestrutura de rede. A gestão de redes é no fundo um serviço que, com auxílio de diversas aplicações, ferramentas e dispositivos, tem o objetivo de auxiliar os gestores de redes, na tarefa de monitorização e manutenção dos diversos pontos que constituem uma rede [11]. A interligação de dispositivos em rede implica a comunicação entre estes, mesmo quando heterogéneos e/ou de fabricantes distintos [9].

O presente capítulo apresenta e descreve aspetos fundamentais da gestão de redes, das funções de gestão (2.1) às arquiteturas de gestão em redes (2.2) e, por fim, as arquiteturas de monitorização centralizada (2.3) e distribuída (2.4), onde serão apresentados os componentes base de cada uma das arquiteturas. Serão descritos modelos de referência e arquiteturas de gestão respetivas, para que o leitor reúna o conhecimento necessário para se contextualizar e perceber o propósito e ligação a cada um dos tópicos abordados.

2.1. Gestão de Redes

Foi já em meados dos anos 80 que surgiu o modelo de gestão de redes denominado *FCAPS* [12]. O termo foi apresentado pela *International Telecommunication Union Telecommunication Standardization Sector (ITU-T), ex-Consultative Committee for International Telephony and Telegraphy (CCITT)*, para auxílio na gestão de redes de telecomunicações e como acrónimo para as 5 funções de gestão padronizadas pela *International Organization for Standardization (ISO)* na gestão de redes de dados*: Fault, Configuration, Accounting, Performance e Security* como representado na *Figura 2.1* [13].

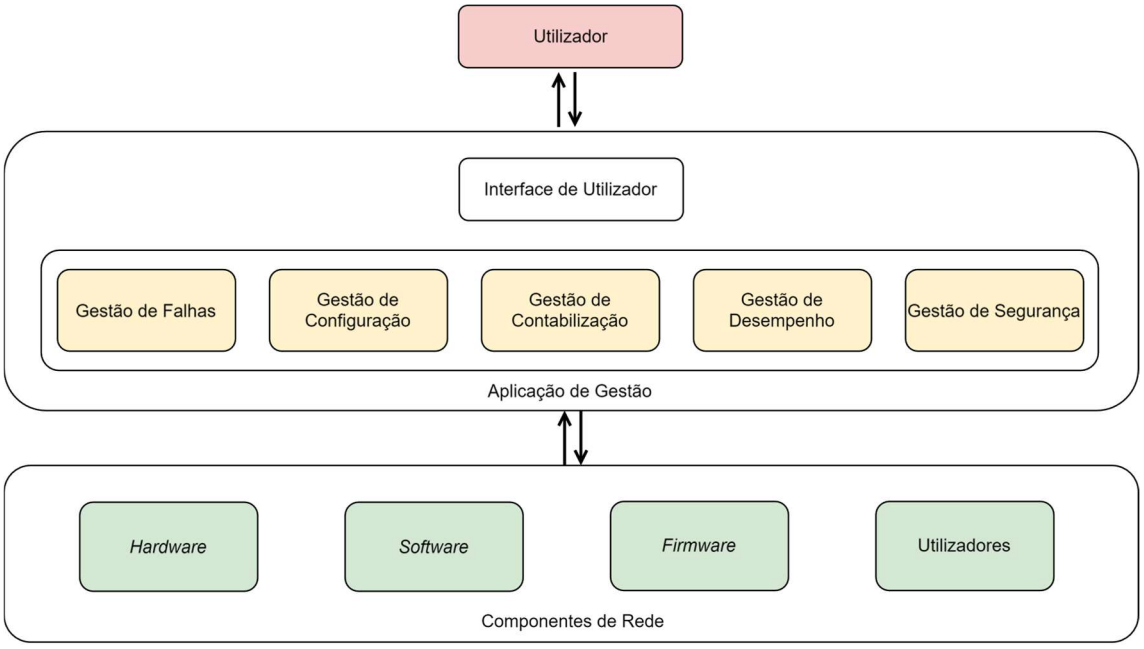

Figura 2.1: Componentes de aplicação de gestão de redes, adaptado de [9].

É através das funções de gestão, e da interação entre elas, que se classifica a informação recolhida pela aplicação de gestão. Esta informação, proveniente de componentes de rede tais como hardware e software, é analisada e apresentada na interface de utilizador mediante a configuração estipulada pelo utilizador.

Existiu a necessidade de universalizar através de normas e especificações como determinados tópicos deverão ser abordados e implementados. Para tal, foram desenvolvidos vários modelos de referência que abordam esta temática, entre os quais o mais reconhecido é o *FCAPS*. Este modelo veio padronizar as cinco funções de gestão mais importantes, *Fault*, *Configuration*, *Accounting*, *Performace* e *Security* [14].

As responsabilidades das funções de gestão estão distribuídas de acordo com o âmbito de cada área funcional, descritas abaixo [15].

- **Gestão de Falhas** (*Fault Management*) – A gestão de falhas é uma das áreas funcionais mais importantes na gestão de redes, permite a deteção de erros através da monitorização e registos de eventos para análise futura. O diagnóstico de erros é feito através duma análise e identificação dos mesmos, a qual permite efetuar uma filtragem de alarmes onde, por sua vez, é possível determinar a causa destes [2]. Caso seja, possível a gestão de falhas pode vir a resolver alguns problemas de forma autónoma [16].

- **Gestão de Configuração** (*Configuration Management*) – A gestão de configuração congrega um conjunto de funções para a recolha e alteração de informação de uma dada configuração de um sistema, mantendo sempre um registo ao longo do tempo, quer a nível de *hardware* ou *software* [2] [8]. A recolha de informação obtida poderá ser usada para a construção de visualizações topográficas da rede, como a obtenção de informação detalhada sobre dispositivos e cablagem, para resolução de problemas recorrentes.

- **Gestão de Contabilização** (*Accounting Management*) – A gestão de contabilização é responsável pelo registo da utilização dos recursos em redes comerciais, com o objetivo de taxar os seus utilizadores e/ou grupos que usufruam destas mesmas. Com base no registo efetuado, é possível obter-se padrões de utilização de recursos, podendo estabelecer políticas e quotas de utilização para grupos ou utilizadores envolvidos [15].

- **Gestão de Desempenho** (*Performace Management*) – A gestão de desempenho congrega as funções de recolha e tratamento de dados sobre o comportamento dos objetos monitorizados. É com base nesses dados obtidos que é feita a análise e deteção de anomalias e previsibilidade, auxiliando assim no processo de tomada de decisões. É essencial no suporte de atividades de configurações para a gestão de falhas e planeamento da rede [17].

- **Gestão de Segurança** (*Security Management*) – A gestão de segurança monitoriza e controla os mecanismos de segurança implementados nos sistemas de gestão da rede. Este define e implementa as políticas de segurança, em zonas críticas onde é efetuada uma análise de risco de problemas de segurança que possam surgir, promovendo a confidencialidade e a integridade dos dados na rede. O levantamento dos requisitos de segurança ajuda na configuração e atribuição de permissões adequadas, na monitorização e registo de situações particularmente relevantes sobre recursos de maior confidencialidade [17] [9].

2.2. Arquiteturas de Gestão de Redes

Foram desenvolvidas várias arquiteturas de gestão de redes sobre as quais serão abordados aspetos importantes referentes às arquiteturas de gestão *OSI, TCP/IP, TMN* e arquitetura de gestão baseada na *Web*.

Uma arquitetura de gestão de redes é essencialmente composta por um sistema, sistema gestor e um sistema gerido. A arquitetura de gestão consolida o modelo Gestor-Agente mostrado na *Figura 2.2*, descreve a interligação entre os elementos e detalha o método de comunicação levado a cabo pelo protocolo de gestão [17].

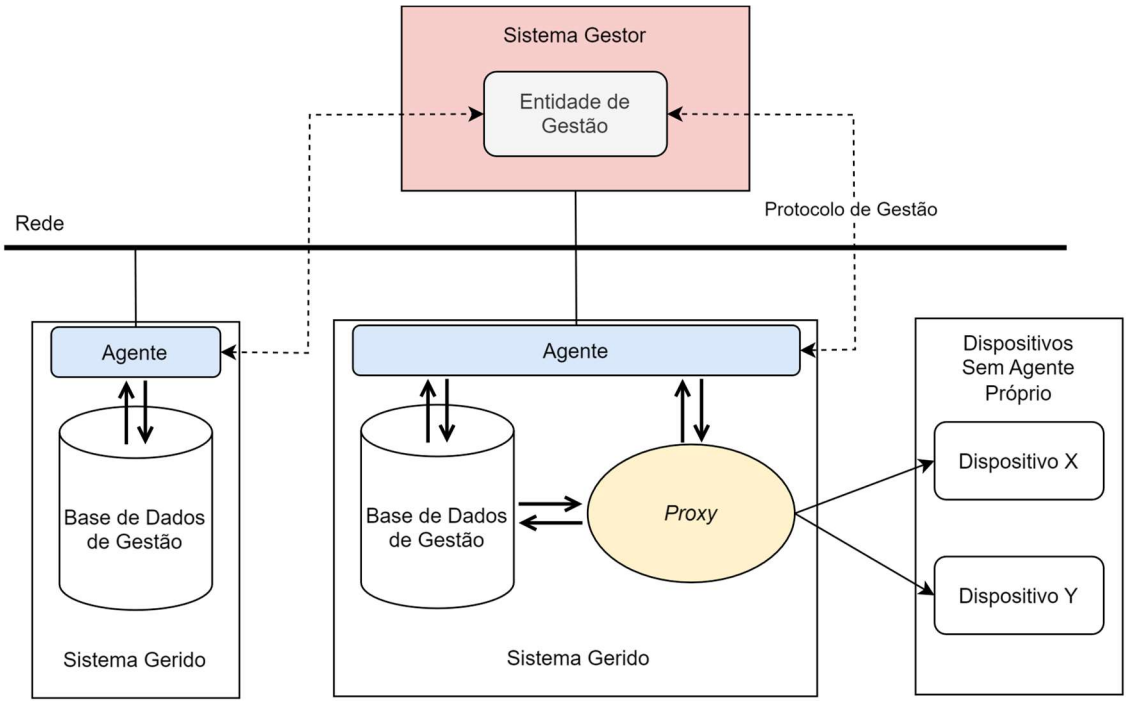

Figura 2.2: Modelo de gestão Gestor-Agente, adaptado de [9].

O sistema gestor é a entidade de gestão que pede dados de interesse aos sistemas geridos, enquanto o sistema gerido é o dispositivo que inclui um agente para fornecer dados e notificar o sistema gestor. Os dispositivos de rede que não implementam protocolos de gestão, são geridos por agentes *proxy*, que traduzem ações do ambiente nativo para o ambiente externo [9].

As arquiteturas de gestão descritas ao longo deste capítulo comportam modelos de informação, modelos organizacionais, modelos de comunicação e modelos funcionais específicos, pelo que o modelo Gestor-Agente engloba nestes quatro sub-modelos de gestão suplementares como representado na *Figura 2.3.*

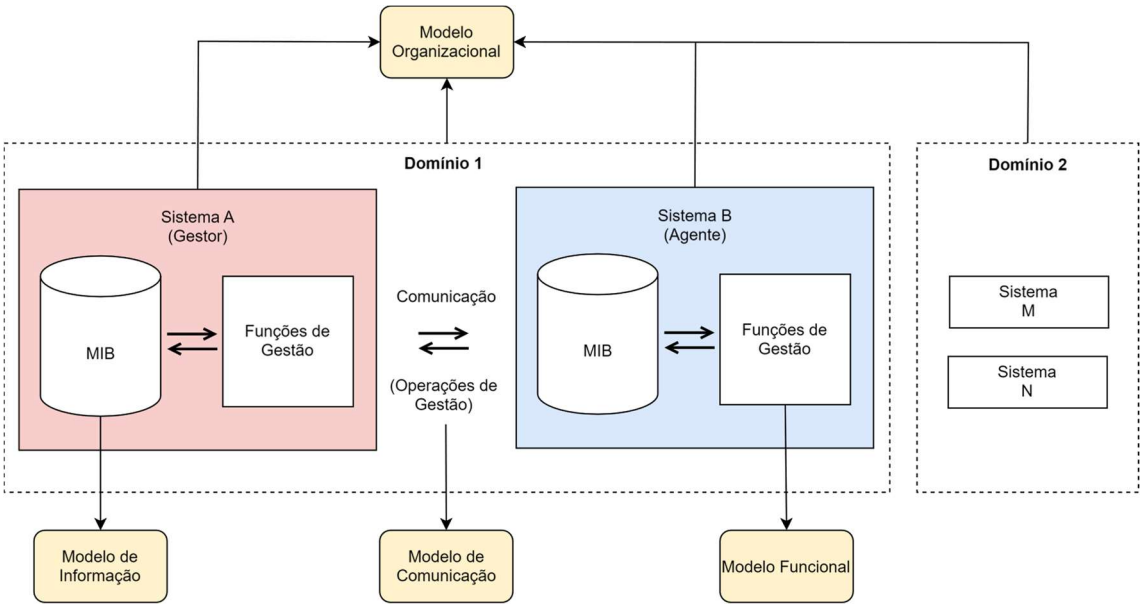

Figura 2.3: Sub-modelos de gestão de redes, adaptado de [9].

O modelo de informação, contém dados para a descrição e modelação dos objetos geridos. Estes dados incluem sintaxe, semântica, definem propriedades e relações, e fazem o mapeamento entre a informação da *MIB* e os recursos por ela descritos [9].

O modelo organizacional define os domínios de gestão e estabelece as responsabilidades intra e interdomínios. Distribui objetos geridos e especifica as responsabilidades e os papeis, como gestor, das entidades de gestão envolvidas. Aqui são considerados aspetos de contabilização, de segurança, aspetos administrativos e políticos.

O modelo de comunicação determina a sintaxe e a semântica de comunicação, e especifica os métodos usados na troca de informação. Aqui, são também definidos os protocolos e serviços disponíveis para a configuração de objetos geridos, abstenção de estados e envio de notificações.

O modelo funcional divide a tarefa de gestão em vários componentes com funcionalidades dedicadas. Descreve os serviços e os objetos geridos relevantes de cada uma das funções de gestão, e identifica a relação estabelecida entre elas para a concretização das funcionalidades esperadas.

2.2.1. Arquitetura de Gestão *OSI*

A arquitetura *Open Systems Interconnection (OSI)* é considerada uma arquitetura de referência lançada pela *Organization for Standardization (ISO)*, a qual permite a comunicação entre diferentes sistemas através de protocolos *standard* [3]. É com base nesta diretiva que a arquitetura de gestão *OSI* surgiu. A arquitetura gestão *OSI*, serve também de base para a arquitetura de gestão *TMN* (*Telecomunication Management Network)* uma arquitetura para gestão distribuída, sendo esta a primeira arquitetura a incorporar os 4 submodelos, e por isso, considerada uma referência arquitetural para a gestão de sistemas em rede [18]. Os 4 submodelos incorporados pela arquitetura *OSI* são o modelo funcional, informação, organizacional e de comunicação [19].

O modelo de informação usa uma abordagem orientada a objetos para modelar os seus recursos relevantes à gestão. Estes são agrupados em classes com outros objetos que partilham os mesmos atributos. A herança permite que um objeto seja uma instância de uma classe ou subclasse de uma ou mais superclasses. Os dados armazenados seguem a notação *Abstract Syntax Notation One (ASN.1)* e constituem a *MIB* local do sistema gerido [20].

O modelo organizacional é baseado numa gestão cooperativa e distribuída, estando interligado com o modelo de comunicação. Neste, o sistema gestor (Gestor) e o sistema gerido (Agente) interagem através de protocolos de gestão para a execução de operações nos objetos geridos [8].

Já o modelo de comunicação é uma representação sistemática, idealizada, do processo de comunicação das arquiteturas de gestão [4]. Este possui 3 áreas de gestão distintas com diferentes tipos de protocolos e serviços de comunicação, gestão de sistemas (*Systems Management*), gestão de camada (*Layer Management*) e operação de camada (*Layer Operation*) [13].

Por fim, o modelo funcional incorpora as 5 áreas funcionais no modelo *FCAPS*, para atender às necessidades específicas da gestão. Identifica, para cada uma das áreas, as funcionalidades, ou seja, o conjunto de funções de gestão de sistema auxiliares relevantes correspondentes [9].

2.2.2. Arquitetura de Gestão *TCP/IP*

A arquitetura de gestão *TCP/IP* serve de base à grande maioria das soluções de gestão para redes e comunicação de dados. Esta arquitetura tem por base o modelo Gestor-Agente, onde o gestor desempenha o papel de cliente e o agente o papel de servidor. É através desta base estipulada, que é feita a troca de informações entre estes, através dos protocolos mais comuns para gestão tais como *SNMP* (*Simple Network Management Protocol*) como podemos ver representado na *Figura 2.4* [9].

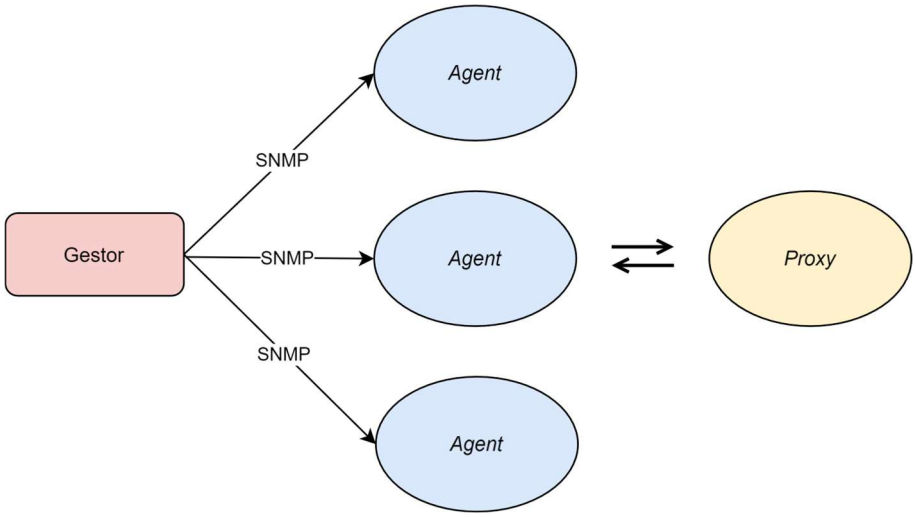

Figura 2.4: Modelo de Gestão *TCP/IP,* adaptado de [9].

Os agentes *proxy*, omissos na arquitetura de gestão *OSI*, permitem a gestão de recursos que não tenham um agente próprio ou que não suportem os mesmos protocolos de comunicação e gestão.

O modelo de informação não segue o paradigma orientado a objetos presente na arquitetura de gestão *OSI*, e não se incorporam modelos organizacional e funcional muito distintos. Este especifica a estrutura genérica da informação de gestão, que está organizada a gestão *MIB*.

A *MIB* representa a árvore de registo que contém os dados de gestão do sistema gerido. Um nó, também conhecido por *Object IDentifier (OID)*, identifica um objeto de gestão.

O modelo de comunicação, assenta no protocolo de gestão *SNMP*, padrão da *Internet*, com três tipos de operações de comunicação: Gestor-Agente, Agente-Gestor e Gestor-Gestor. Na comunicação Agente-Gestor, o agente notifica ao gestor a ocorrência de situações particularmente relevantes com *traps* sem solicitação prévia. A comunicação Gestor-Agente, o gestor acede à *MIB* do agente para consultar ou modificar objetos geridos. A modificação de objetos geridos é levada a cabo pelo agente, que indica o resultado das operações pedidas.

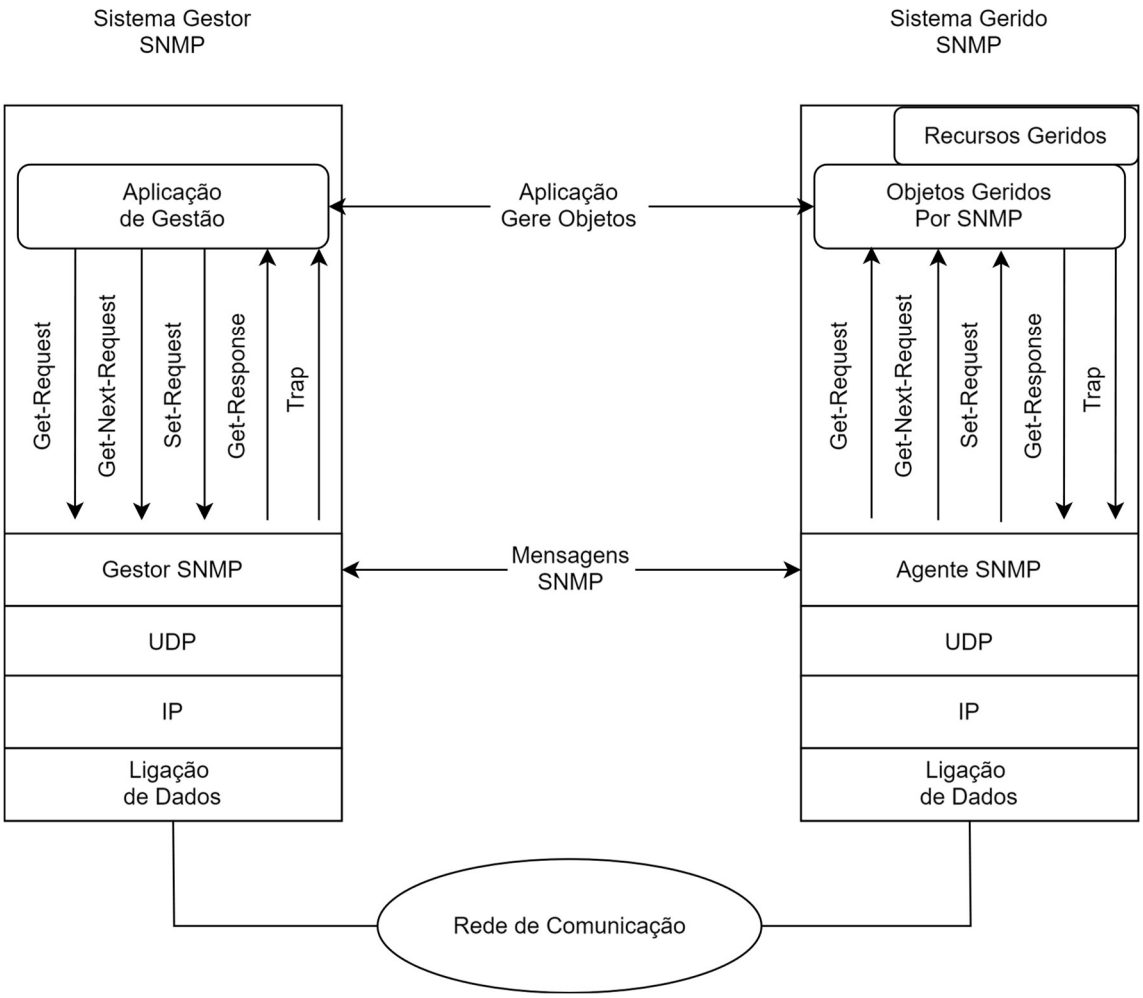

Figura 2.5: Arquitetura do protocolo *SNMP,* adaptado de [9].

As mensagens *SNMP* contêm um cabeçalho e um *Protocol Data Unit (PDU)*. O cabeçalho especifica a versão do protocolo e o nome da comunidade *SNMP* para autenticação. A *PDU* está associada à comunicação, com formato e conteúdo diferente para cada operação.

A primeira versão, *SNMPv1*, dispõe das 4 operações *Get-Request*, *Get-Next-Request*, *Set-Request* e *Trap*. A segunda versão, *SNMPv2*, permite ao Gestor desempenhar o papel de Agente e ao Agente desempenhar o papel de Gestor, em interações devidas. É mais seguro, oferece um modelo de informação com suporte para novos tipos de dados, e um modelo de comunicação com suporte para as duas novas operações *Get- Bulk-Request* e *Inform-Request*. A terceira versão, *SNMPv3*, resolve as questões de seguranças adiadas pelas versões precedentes dado que as tecnologias propostas para *o SNMPv2* não se revelaram totalmente seguras [5].

2.2.3. Arquitetura de Gestão *TMN*

A arquitetura de gestão *TMN* foi desenvolvida nos anos 80 e teve como principal objetivo possibilitar a gestão integrada e homogénea de um conjunto heterogéneo de redes, que normalmente compõem as redes utilizadas por operadoras de comunicação [9]. Este tipo de arquitetura permite proporcionar uma estrutura de rede organizada com interligação de diversos tipos de sistemas de administração, operação e manutenção, em equipamentos de telecomunicações, usando uma arquitetura *standard* e interfaces normalizados.

Esta é baseada no conceito de "*Overlay Network*", onde a gestão de redes de telecomunicações é efetuada através de uma rede de gestão distinta à qual possui suporte para uma gestão integrada. O facto de este tipo de gestão possuir uma hierarquia de gestão faz com que esta possua um fluxo de informação específico e previsto, como podemos verificar na *Figura 2.6*.

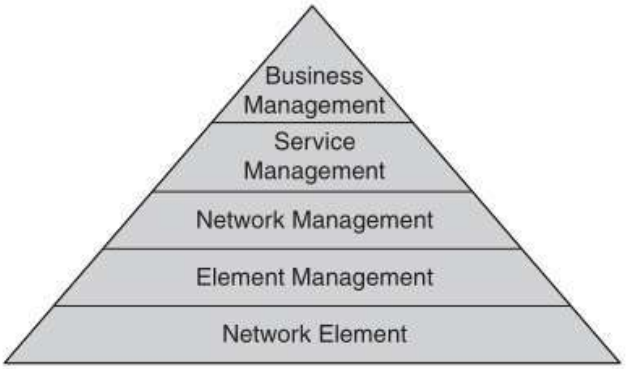

Figura 2.6: Hierarquia da arquitetura de gestão *TMN,* adaptado de [9].

As fatias inferiores da pirâmide concentram funções de gestão mais granulares, e as fatias superiores comportam funções de gestão tangentes às grandes linhas de ação do operador de telecomunicações [17].

A gestão dos elementos de rede (*Element Management*) monitoriza o nível de desempenho dos elementos de rede. A informação recolhida é armazenada numa base de dados e analisada por funções de gestão de nível superior.

A gestão de rede (*Network Management*) comporta aspetos de conectividade, desempenho, encaminhamento da informação, congestão e falhas de rede.

A gestão de serviços (*Service Management*) é responsável por construir, monitorizar e manter serviços procurados pelos utilizadores. A gestão de utilizadores, a contabilização de recursos e a qualidade se serviço contratada são aspetos de interesse neste nível de gestão.

Por fim, a gestão de negócio (*Bussiness Management*) envolve decisões que afetam o desempenho do negócio. Aqui temos a análise de custos e lucros, análise de adesão e análise de serviços bem conseguidos.

2.2.4. Arquitetura de Gestão Baseada na *Web*

A arquitetura de gestão baseada na *web* utiliza os *web browsers* como terminais de gestão. Utilizar-se os *webs browsers* como consolas de gestão trouxe uma maior facilidade de se poder aplicar funções de gestão, em qualquer lugar sobre qualquer plataforma. Existem dois tipos de abordagens para uma gestão baseada na *web,* a abordagem integrada e abordagem com *proxy*.

A abordagem integrada para gestão baseada na *web,* representada na *Figura 2.7,* é útil para redes de pequena dimensão, pois evita a utilização de uma plataforma de gestão com o propósito de auxiliar nas atividades de gestão [1].

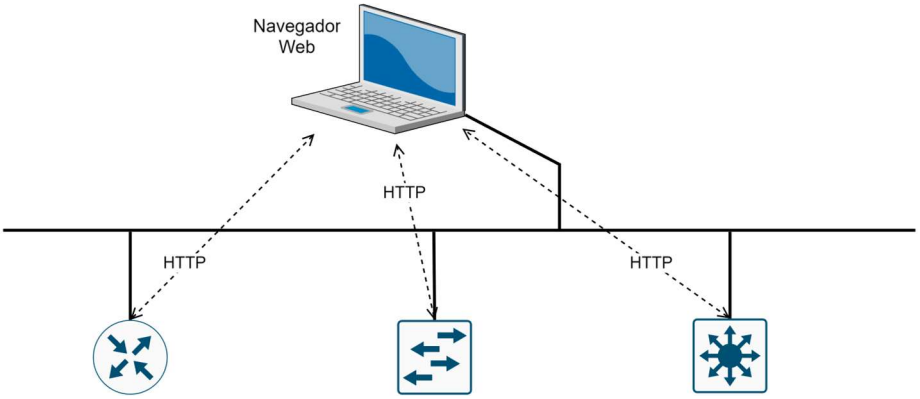

Figura 2.7: Abordagem integrada para gestão baseada na *Web,* adaptado de [9].

A abordagem com *proxy* para gestão baseada na *web*, representada na *Figura 2.8* é útil para redes de maior dimensão, com dispositivos centralizados responsáveis por recolher, correlacionar e processar grande volume de dados.

Os dispositivos centralizados responsáveis por recolher, correlacionar e processar grande volume de dados, comportam custos, mas substituem ferramentas de gestão tradicionais com uma plataforma de gestão complexa, robusta e completa.

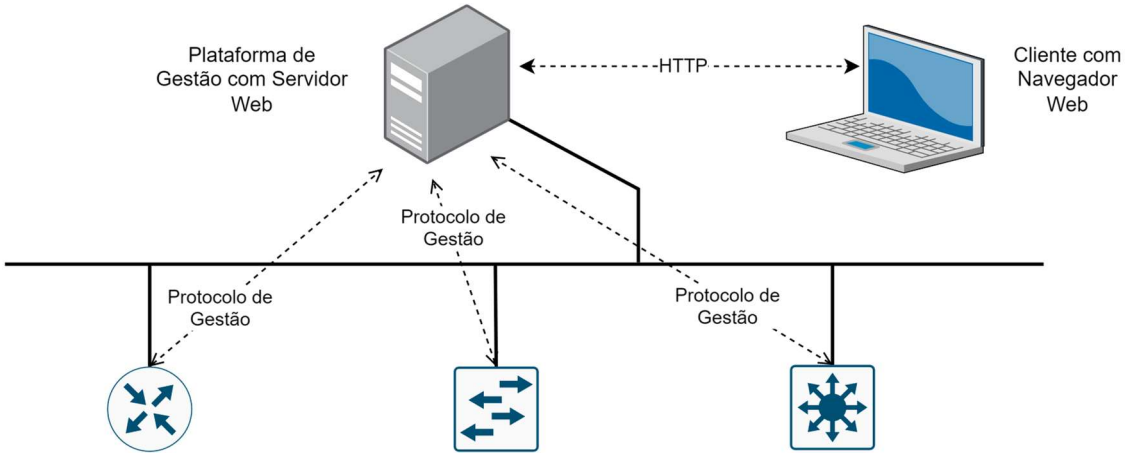

Figura 2.8: Abordagem com *proxy* para gestão baseada na *web*, adaptado de [9].

2.3. Arquiteturas de Monitorização Centralizadas

As primeiras arquiteturas de monitorização de serviços e infraestruturas de redes, tinham por base um sistema centralizado, onde um único ponto ficaria responsável pelos processos de recolha e tratamento de informação de toda infraestrutura e serviços [11]. Estes processos de recolha e análise de informação têm por base as funções de gestão referidas anteriormente, com a utilização de protocolos *standard* para monitorização de sistemas e redes de uma dada infraestrutura [21]. Esta arquitetura é composta por uma máquina, tipicamente um servidor dedicado, para monitorização dos serviços e infraestruturas de rede [22]. Na *Figura 2.9*, tem-se a representação de uma arquitetura centralizada genérica, que representa o ponto central, onde se dá o processamento, recolha e tratamento das métricas duma dada infraestrutura [23].

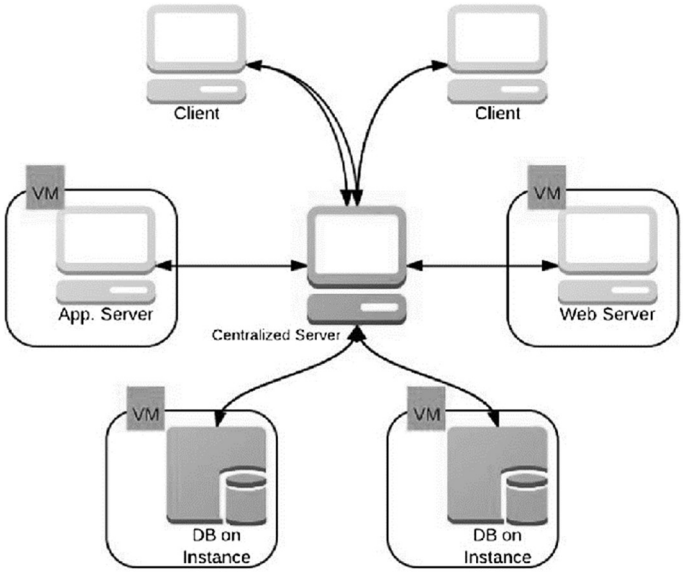

Figura 2.9: Arquitetura monitorização centralizada genérica.

A arquitetura de monitorização centralizada é comumente utilizada devido à sua simplicidade de implementação e manutenção. Contudo, esta é considerada ineficiente a nível de escalabilidade [24]. Com a expansão nas últimas décadas nas áreas das Tecnologias de Informação (TI), esta arquitetura demostrou possuir grandes limitações, no que toca à sua escalabilidade e fiabilidade para ambientes e serviços que têm por base sistemas distribuídos [25] [10] [26].

2.4. Arquiteturas Monitorização Distribuídas

As arquiteturas de monitorização distribuídas são fortemente utilizadas em *cloud providers*, devido às suas características próprias, de serviços e infraestruturas [27]. Como afirmado inicialmente, uma falha na rede ou num serviço implica perdas de produção e, consequentemente enormes custos financeiros [28]. Este problema é um dos principais motivos, pelos quais a monitorização das infraestruturas de *cloud* [29] são fundamentais para a garantia da qualidade do serviço aos seus utilizadores [30]. As arquiteturas de monitorização distribuídas surgiram devido à necessidade de evolução dos mecanismos de monitorização, face à expansão das redes de dados [31]. Estas arquiteturas têm demonstrado grandes capacidades de escalabilidade, no que toca ao balanceamento de grandes fluxos de dados e informação, tornando a tarefa de monitorização consequentemente mais complexa [29] [30].

Uma arquitetura de monitorização distribuída caracteriza-se pela dispersão da monitorização dos serviços e da infraestrutura de rede, com máquinas designadas por *proxies*, como representado na *Figura 2.10* [32]. Estes elementos da arquitetura de monitorização são posicionados em diversos pontos chave da infraestrutura, responsabilizando-se por funções de monitorização específicas e definidas pelo administrador, adequadas à zona de rede e serviços a monitorizar [21].

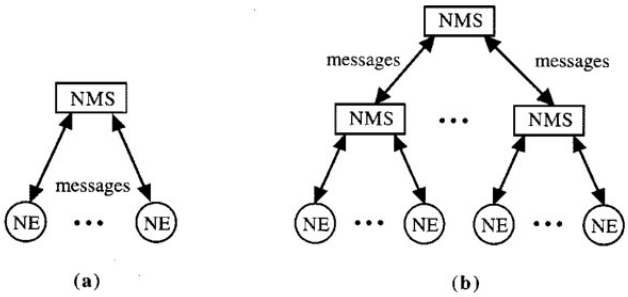

Figura 2.10: Comparação de arquitetura centralizada(a) e distribuída(b), retirado de [33].

Desta forma, os processos de recolha e análise dos dados de monitorização são mais flexíveis, escaláveis e/ou distribuídos [34]. A flexibilidade e agilidade na gestão de todos estes mecanismos em simultâneo, permite aplicar configurações a vários serviços de monitorização de uma forma agilizada, podendo aplicá-las a tipos de equipamentos físicos, ou até mesmo a infraestruturas de rede geograficamente distintas [33] [35].

Dependendo da dimensão da organização e serviços, podem possuir a segmentação além de pontos da rede específicos, como na camada aplicacional. Esta abordagem é muito comumente utilizado em *cloud providers* [10] onde, devido à enorme quantidade de redes privativas internas e externas, é utilizada uma monitorização que percorre até à camada aplicacional, para seus utilizadores e serviços [36] [31]. Este tipo de abordagem permite criar mecanismos de monitorização [37] mais robustos, devido à forma segmentada como a monitorização está a ser efetuada [38].

Em [8], os autores propõem uma solução para a monitorização distribuída em redes definidas por *SDN* (*Software-defined networking*) através da telemetria *in-band*, onde os dados de monitorização são obtidos diretamente nos dispositivos da rede, em vez de serem transmitidos para um ponto central.

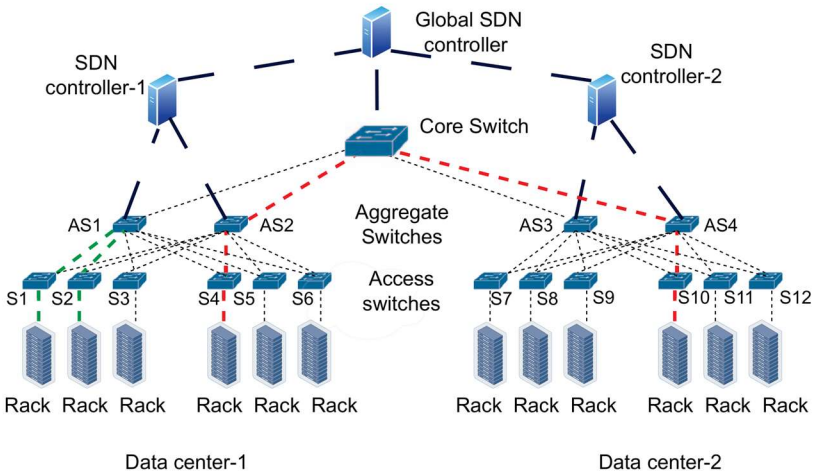

Figura 2.11: Telemetria de rede *In-Band* distribuída hierarquicamente por SDN controlo, retirado de [35].

Para superar as limitações da telemetria tradicional em banda, é proposta uma abordagem de *INT (In-band network telemetry)* distribuída hierarquicamente. Esta solução utiliza o *data plane* centralizado lógico, como o *Software Defined Networking (SDN)*, para distribuir tarefas de processamento e análise da *INT* entre múltiplos *switches*, garantindo monitorização de redes mais escalável e eficiente. A *Figura 2.11* mostra duas linhas a vermelho e a verde, onde ambas mostram o processamento ao nível de *data plane*, enquanto a azul mostra as atualizações a nível do *data plane*.

No [39], os autores apresentam uma arquitetura de monitorização de redes definidas por *SDN* (*Software Defined Network*), baseada no controlador *ONOS* (*Open Network Operating System*), utilizando a telemetria *In-band (INT).* A *INT* permite a recolha de informações detalhadas sobre o estado da rede, diretamente do *data plane*, proporcionando monitorização em tempo real e de alta granularidade.

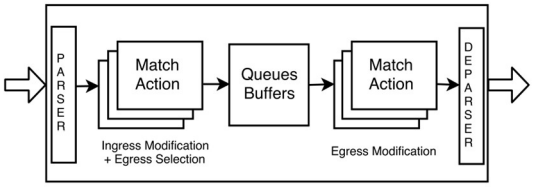

Figura 2.12: Arquitetura *switch P4*.

A implementação desta arquitetura no *ONOS*, combinada com dispositivos programáveis através da linguagem *P4*, permite a recolha e análise de dados de monitorização em tempo real. Isso possibilita a deteção de eventos e anomalias na rede, de forma mais ágil e precisa, melhorando a capacidade de resposta e a gestão da infraestrutura de rede.

2.5. Conclusão

Neste capítulo, foram apresentados e descritos os aspetos fundamentais da gestão de redes, as áreas funcionais *FCAPS*, o modelo de gestão Gestor-Agente e as arquiteturas de gestão *OSI*, *TCP*/*IP*, *TMN* e a arquitetura de gestão baseada na *web* [18].

As arquiteturas de gestão consolidam o modelo Gestor-Agente, análogo à arquitetura cliente-servidor. A arquitetura de gestão *OSI* foi a primeira a incorporar os submodelos referidos anteriormente, nomeadamente modelo de informação, modelo organizacional, modelo comunicacional e, por fim, modelo funcional [9]. Esta serviu de base para a definição de outras arquiteturas de gestão. A arquitetura de gestão *TCP/IP*, referência nas soluções de gestão para redes de comunicação de dados, suporta agentes *proxy* para gestão de recursos sem agente próprio ou que não suportem os mesmos protocolos de comunicação e gestão. A arquitetura de gestão *TMN* tem como objetivo a gestão homogénea de redes heterogéneas comuns nas áreas das comunicações [40].

A diferenciação entre arquiteturas de monitorização de redes centralizadas e distribuídas, baseia-se principalmente em aspetos como desempenho, escalabilidade, tolerância a falhas e complexidade de implementação.

Na arquitetura centralizada, o desempenho pode ser limitado pela capacidade do servidor central. A falha no servidor central, pode resultar na perda de monitorização, pois todos os dados e processos dependem de um único ponto. Isso cria um ponto de falha único, tornando a monitorização vulnerável a interrupções. É geralmente mais fácil de implementar e gerir, pois a monitorização e o controle são realizados em um único ponto, o que simplifica a configuração e a manutenção. Possui desafios de escalabilidade, onde à medida que o número de dispositivos na rede cresce, o servidor central precisa de mais capacidade de processamento e armazenamento.

Por outro lado, a arquitetura distribuída permite o processamento local em várias instâncias ou nós de monitorização, reduzindo a carga em qualquer ponto. É inerentemente escalável, pois permite que novos nós de monitorização sejam adicionados conforme necessário, melhorando latência e a capacidade de resposta, essencial para redes dinâmicas e de grande porte [41] [9]. Mesmo que um nó de monitorização falhe, os outros podem continuar a operar, garantindo uma continuidade de serviço de monitorização. Por sua vez, requer uma coordenação mais complexa entre os nós, especialmente em relação à sincronização de dados e à consistência das informações, aumentando a sua complexidade de implementação e gestão.

O próximo capítulo irá descrever e detalhar a problemática existente em torno da infraestrutura e serviços da instituição Governamental, e, irá especificar os requisitos que servirão para a proposta de arquitetura de monitorização para a instituição Governamental.

3. Análise da Rede Institucional

Este capítulo propõe-se a descrever e analisar a rede institucional que suporta os serviços e as aplicações utilizadas e desenvolvidas da instituição Governamental. Pretende, ainda, caracterizar os problemas identificados e os desafios para uma monitorização completa da rede e dos sistemas de informação.

A instituição Governamental providenciou o desenvolvimento dos serviços digitais nas últimas décadas e, tendo sob a sua responsabilidade o suporte a uma população de mais de 250 mil pessoas, integra nos seus quadros quase 5 milhares de funcionários, a operar em centenas de locais espalhados geograficamente por duas ilhas atlânticas. Pode-se, então, considerar que esta possui uma infraestrutura tecnológica de envergadura considerável, podendo estar na categoria de grande empresa/instituição.

Esta infraestrutura pode-se ainda considerar como sendo bastante heterogénea, constituída por múltiplas entidades de natureza e necessidades diferenciadas, desde secretarias regionais a escolas primárias, básicas e secundárias, centros cívicos, institutos públicos, entre outros mais, dispersos geograficamente ao longo de duas ilhas. A cada local específico, designado de *site*, existe uma ligação exclusiva e dedicada, onde a interligação com outos *sites* da rede fornecida por um operador contratado pela instituição Governamental. O acesso à *Internet* é efetuado, através por outro fornecedor de serviços de interligação à *Internet*.

Os serviços prestados, direta e indiretamente, às populações das ilhas, é efetuado pelas suas diversas entidades dispersas ao longo da região, onde se utiliza tal como referido anteriormente uma rede interna dedicada para comunicação entre estas, bem como utilização de diversos serviços a partir dos *datacenters* da instituição Governamental. Quando existe uma falha na rede, determinados serviços deixam de poder estar disponíveis tanto aos seus próprios utilizadores bem como à população, sendo que este tipo de falhas implica custos e redução de produtividade e, é nestas situações, que a monitorização dos vários serviços de uma rede é necessário.

A apresentação anterior pretendeu descrever sucintamente a dimensão geral da rede institucional da entidade Governamental, referindo algumas das suas particularidades e ajudando a melhor compreender o contexto do problema. De seguida, as próximas secções pretendem adicionar detalhes sobre os vários *sites* da instituição Governamental (3.1), a forma como estes se encontram interligados (3.2), quais os serviços aplicacionais utilizados na instituição (3.3), quais as características dos seus *datacenters* (3.4) e sua atual monitorização (3.5) e, por fim, a elaboração dos requisitos para a proposta de arquitetura de monitorização (3.6).

3.1. Descrição dos *Sites* da Instituição Governamental

Os sites da instituição Governamental, tal como referido anteriormente, são bastante heterogéneos, ou seja, de dimensões e forma de utilização de rede muito distintas, e encontram-se espalhados geograficamente ao longo da região, sendo que, à data de maio de 2024, existiam cerca de 265 *sites*. Uma forma de categorizar cada um destes *sites* é pela orgânica institucional e podem ser segmentados da seguinte forma: serviços, institutos, escolas, conservatório e formação. A sequência apresentada foi dos *sites* de maior dimensão para os de menor dimensão, onde na *Figura 3.1,* acrescenta-se a informação da quantidade de *sites* por grupo.

Figura 3.1: Distribuição dos *sites* da instituição Governamental.

Estas entidades possuem características próprias e distintas umas das outras de acordo com a natureza das suas funções, com um total aproximadamente de cinco mil funcionários no quadro da função pública regional. As principais diferenças entre estes *sites* são essencialmente os tipos de serviços que possuem, como o acesso à *internet* é efetuado e a disponibilização de equipamentos aos seus utilizadores.

O utilizador normal da instituição Governamental possui um computador de trabalho e um telefone *VoIP (Voice over Internet Protocol)* associado, possui de igual modo acesso ao sistema de impressão como também *ao sharePoint* para consulta de documentos. O acesso à *Internet* de cada um dos *sites* da instituição é via a rede dedicada que interliga os *datacenters* da entidade Governamental que, por sua vez, disponibilizam vários *links* de acesso à *internet* a partir destes. Existem determinados *sites*, como é o caso das escolas secundárias e conservatórios, onde face às suas necessidades especiais, possuem circuitos de *internet* locais e, nestas situações, é por esta via que o acesso é efetuado. De igual modo, existem determinados *sites* que face à natureza Governamental possuem a sua independência na aquisição de equipamentos, fator este que permite que estes *sites* equipam os seus utilizadores, como é o caso dos institutos.

3.2. Rede e Interligação

A instituição Governamental possui uma rede interna exclusiva e dedicada que interliga todos os *sites* aos seus *datacenters*, permitindo assim o acesso a recursos partilhados entre todos estes. Esta rede interna é designada por rede privativa da instituição Governamental, possuindo vários agregadores espalhados ao longo das ilhas, que se interligam aos dois *datacenters* da instituição Governamental através de dois *routers* industriais.

Todos os 265 *sites* da instituição Governamental possuem um *router* onde interliga pelo menos a um dos agregadores referidos anteriormente. Existem dois tipos de *routers* nos *sites* da instituição Governamental, um destes possui apenas uma ligação a um agregador, e o outro possui duas ligações a dois agregadores distintos por questões de redundância. Os locais que possuem o *router* com redundância aos agregadores da rede privativa são, tipicamente, locais que possuem mais de cem utilizadores.

A comunicação de toda a rede privativa é efetuada através do protocolo de *routing BGP (Border Gateway Protocol),* que interliga aos *datacenters* da instituição Governamental.

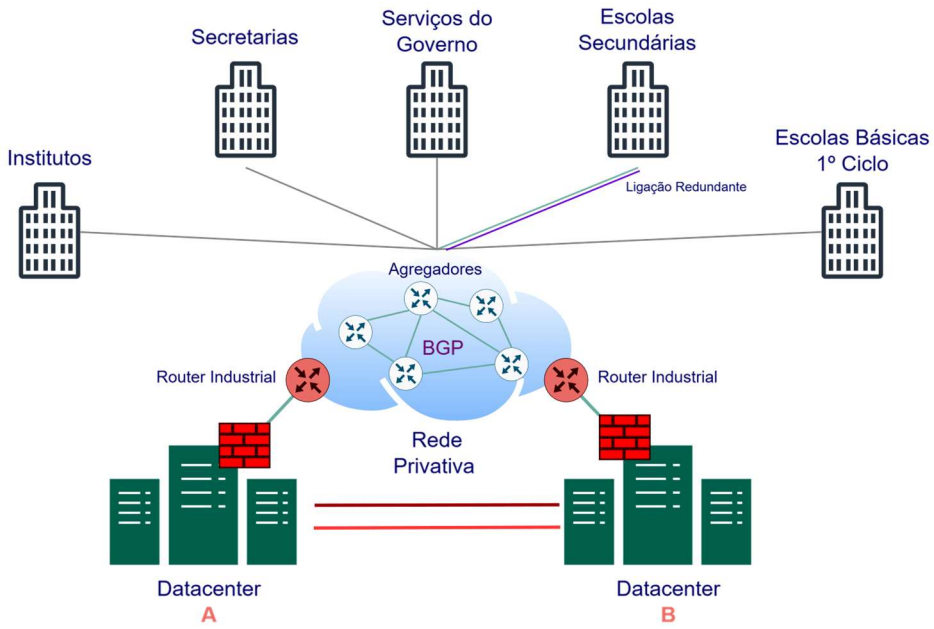

Figura 3.2: Infraestrutura da rede privativa da instituição Governamental.

A *Figura 3.2* representa, de modo geral, a arquitetura da infraestrutura de rede da instituição Governamental, sendo constituída por dois *datacenters* que albergam toda a infraestrutura e serviços da instituição. As linhas vermelhas representam a comunicação bidirecional entre os *datacenters* suportada por fibras escuras e dedicadas com finalidade de garantir alta disponibilidade.

Os *routers* industriais presentes em cada um dos *datacenters* da instituição Governamental, *Figura 3.3,* recebem todas as ligações dos vários agregadores espalhados ao longo das ilhas. Estes *routers* interligam por sua vez ao *router* / *firewall* do *datacenter* da instituição Governamental e, é a partir desta, que são efetuadas as verificações de segurança de toda a instituição. A arquitetura da rede privativa foi projetada para alta disponibilidade onde em caso de falha de um dos *datacenters* é efetuada automaticamente a comutação das comunicações para o *datacenter* disponível. Apesar da rede privativa ser propriedade da instituição Governamental, a sua gestão e monitorização é da responsabilidade de um provedor de serviços externo.

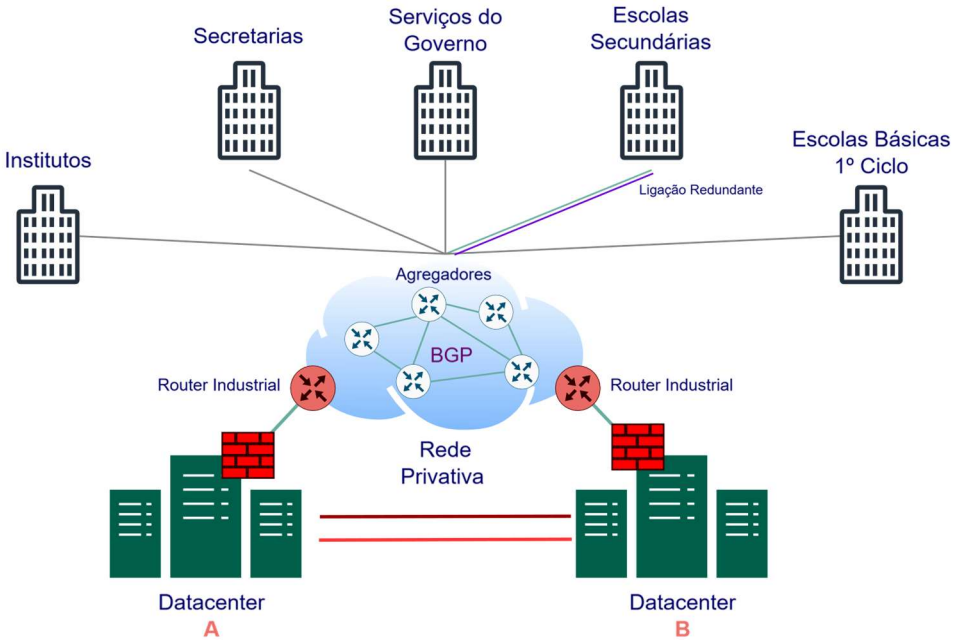

Figura 3.3: Arquitetura de interligação da rede privativa aos *datacenters*.

Nos equipamentos *routers* / *firewalls* da instituição Governamental tem-se o registo da quantidade de tráfego existente e quais as suas horas de maior consumo dos recursos nos *datacenters.* Tem-se registado os maiores picos de largura de banda, que cresce, de uma forma exponencial cresce a partir das 8 horas da manhã até às 12:30 horas, com registo de maior consumo entre as 11 horas e as 12 horas da manhã, na ordem dos *2Gbps* como podemos verificar na *Figura 3.4*.

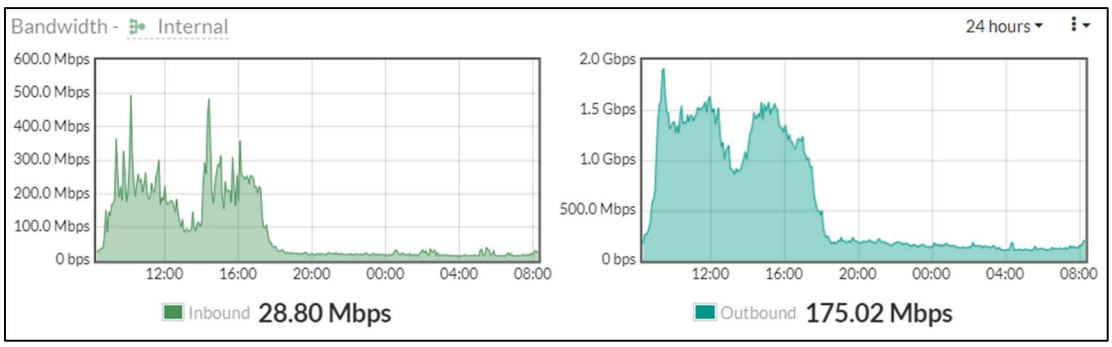

Figura 3.4: Largura de banda dos equipamentos *routers* / *firewall* nas últimas 24 horas.

Todo este tráfego advém, além dos dois *datacenters* da instituição Governamental, dos cerca 265 *sites* remotos existentes que utilizam a rede privativa.

Tal como os registos de largura de banda, possui-se também registo do número de sessões estabelecidas que, em média, rondam as 300 mil sessões, nas horas de maior utilização dos recursos da rede privativa da instituição Governamental. A *Figura 3.5* mostra a evolução do número de sessões *TCP* estabelecidas nas últimas 24 horas num dia de semana do mês de agosto.

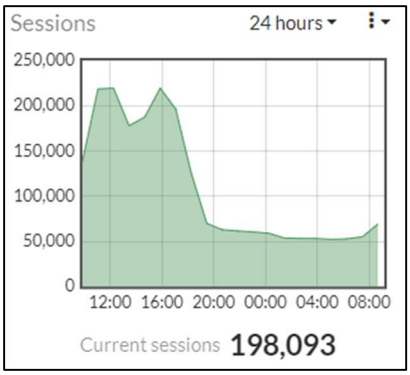

Figura 3.5: Número de sessões *TCP* estabelecidas nas últimas 24 horas.

O acesso à *internet* dos *sites* da instituição Governamental é efetuado através dos *datacenter*, que recebem todas as ligações da rede privativa e, através de regras de *SD-WAN* (*Software-Defined Wide Area Network),* encaminha-as para a *Internet.* Estas regras são definidas com base no tipo de rede ou na camada aplicacional, de maneira a garantir uma melhor utilização dos recursos no acesso à *internet*. Pode-se dar como exemplo a utilização de *links* de *Internet* específicos para a utilização de manuais digitais nas escolas da instituição.

Face à criticidade de acesso à *Internet*, nos *datacenters* da instituição Governamental existem vários circuitos de acesso à *Internet,* de *ISP* (*Internet Service Provider*) distintos, garantindo desta forma alta disponibilidade inclusive no acesso à *internet* de toda a instituição Governamental.

(Espaço deixado em branco propositadamente)

3.3. Serviços Aplicacionais

A instituição Governamental possui uma enorme diversidade de serviços, onde a vasta maioria passa pela gestão e disponibilização de armazenamento recorrendo a serviços de partilhas de ficheiros, pela disponibilização de recursos para programas e serviços governamentais para disponibilização pública, entre outros mais. Face à sua natureza Governamental, existe a preocupação de garantir a integridade e confidencialidade da informação disponibilizada e armazenada. Esta diversidade de serviços e entidades dispersas geograficamente pelas ilhas, apresentam uma complexidade acrescida.

Existem serviços básicos comuns na vasta maioria dos *sites* da instituição Governamental como é o caso sistema de telefone *VoIP (Voice over Internet Protocol)* e sistema de impressão centralizado.

3.4. *Datacenters*

A instituição Governamental possui dois *datacenters* que albergam toda a sua infraestrutura, designados por *datacenter A* e *datacenter B*. De maneira a garantir a alta disponibilidade e questões de redundância, os *datacenters* possuem mecanismos de sincronização entre estes, permitindo o funcionamento de toda infraestrutura da instituição Governamental somente com um dos *datacenters* ativo. A ligação entre todos estes pontos da infraestrutura é estabelecida através da sua rede privativa, com ligações exclusivas, não partilhadas por operadores *ISP (Internet Service Provider)*, incluindo as respetivas ligações entre o *datacenter A* e *datacenter B*. Ambos *datacenters* possuem diversos equipamentos, nomeadamente: servidores dedicados para virtualização; *routers*; *switches*; e *storage* para armazenamento de dados, que tem por base a arquitetura de hiper convergência. Possuem serviços de operadores para acessos à *internet* como também das comunicações telefónicas, mais concretamente os *SIP Trunks* (*Session Initiation Protocol Trunking*) de diversos *ISP (Internet Service Provider)* distintos.

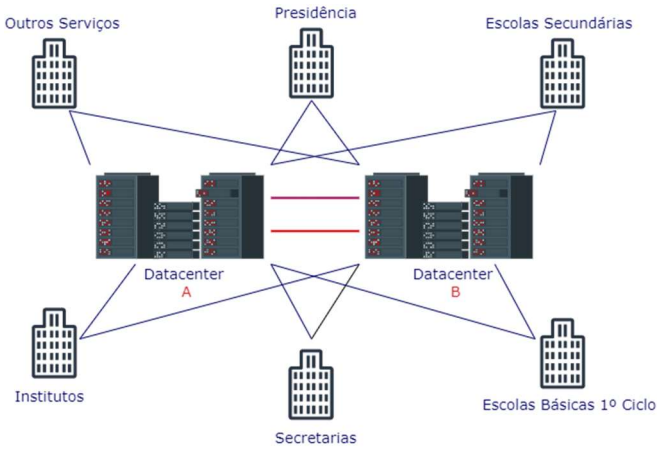

Figura 3.6: Esquema geral dos *datacenters* da instituição governamental.

3.5. Monitorização da Instituição Governamental

Face à envergadura da infraestrutura da instituição Governamental, podemos afirmar que esta é considerada uma rede de tamanho considerável dispersa ao longo das ilhas atlânticas. Esta característica enfatiza a complexidade na sua monitorização, desde a camada física à aplicacional. O facto de esta possuir serviços heterogéneos ao longo de diversas entidades de natureza e fins distintos, realça a heterogeneidade existente em toda a organização. A instituição Governamental até recentemente apenas possuía mecanismos de monitorização básicos que, na sua maioria, passavam por obter o *status code* de alguns *websites* de maior importância para a instituição. As monitorizações dos d*atacenters* da instituição Governamental eram quase inexistentes. Na grande maioria das vezes, os administradores de sistemas e redes só sabiam efetivamente de alguma situação anómala quando os utilizadores reportavam a existência de serviços indisponíveis.

A monitorização existente baseava-se, muitas vezes, na deteção por parte do utilizador, e através do seu sistema interno de pedido de assistência técnica. Assim, o problema era devidamente detetado e, por sua vez, intervencionado. A *Figura 3.7* mostra o programa interno da instituição Governamental, a que os seus utilizadores recorrem.

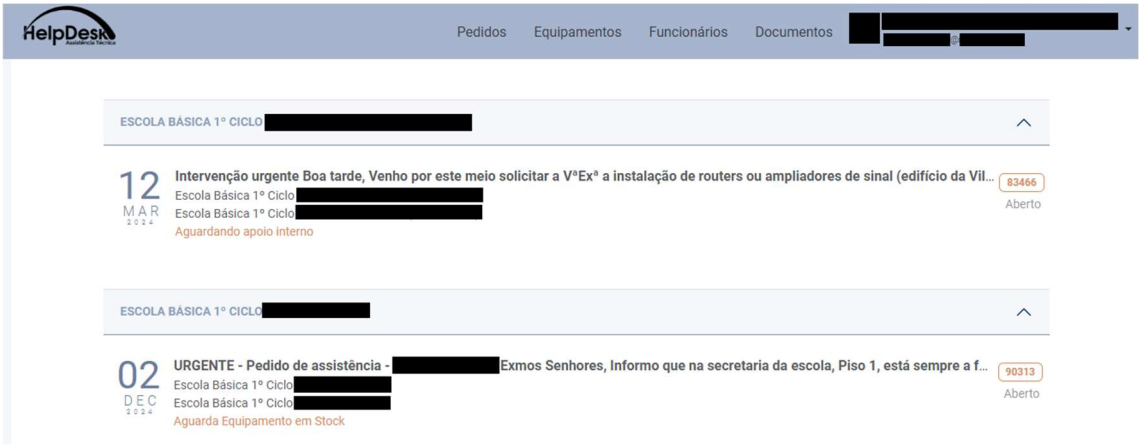

Figura 3.7: Sistema de pedido de assistência da instituição Governamental.

As monitorizações dos equipamentos presentes nos *datacenters* da instituição Governamental eram monitorizadas pelos administradores de sistemas e redes, efetuando *login* nos próprios equipamentos e analisando os *logs,* confirmando se o equipamento está operacional ou não. Este método não é considerado produtivo, visto possuir-se centenas de equipamentos em cada um dos *datacenters,* e ser um processo monótono e moroso.

Existem serviços correlacionados com a área administrativa, que, face à inexistência de monitorização, traziam perda de produtividade para os seus utilizadores, por exemplo quando o sistema de impressão aquando ficava indisponível, entre outros.

3.6. Especificação dos Requisitos

Tendo em consideração o que foi referido ao longo deste capítulo, note-se a importância da adoção de um modelo de gestão de redes e sistemas, que auxilie o gestor de sistemas e redes, na execução e monitorização da rede da instituição Governamental, a fim de garantir e melhorar a qualidade dos serviços prestados a todos os seus utilizadores.

Devido às características próprias da infraestrutura da instituição Governamental, a solução deverá permitir a centralização da gestão dos vários equipamentos e serviços que constituem a rede da instituição e, ao mesmo tempo, permitir a implementação distribuída do sistema de monitorização, face às suas características próprias da sua rede. Esta diversidade de serviços e entidades dispersas geograficamente ao longo das ilhas, apresentam uma complexidade na sua monitorização, apresentando grandes flutuações devido à forma dispersa como estes serviços estão ao longo da região. A solução integrada terá de possuir um conjunto de características base, que complementam as fragilidades identificadas na rede da instituição Governamental, sendo essas características a fiabilidade, robustez e escalabilidade. Este último ponto é deveras crítico, pois a solução terá de suportar uma vasta diversidade de equipamentos e serviços, com características próprias e protocolos próprios.

A solução integrada terá de possuir uma forte componente de previsibilidade e alarmística, permitindo assim o envio de notificações aos gestores de sistemas e redes aquando existe alguma falha na rede, tornando assim a sua intervenção mais célere e eficaz, diminuindo tempos de indisponibilidade de determinados serviços. A previsibilidade é também um ponto deveras importante, pois tendo em conta os *standards* na monitorização de uma rede atualmente, a solução integrada deverá prever determinados problemas na rede e notificar o gestor, antes que estes de facto aconteçam.

Será necessário permitir a monitorização dos *datacenters* da instituição Governamental, onde de uma maneira central, terá de ser possível ter-se a noção geral de todos os equipamentos constituintes de ambos *datacenters,* como também possuir-se uma noção da escalabilidade dos recursos existentes. Este último ponto é deveras importante, pois irá permitir à instituição Governamental planear atempadamente a aquisição de recursos para os *datacenters*, tendo por base a monitorização existente, garantindo desta forma, capacidade de escalabilidade para novos serviços e projetos.

3.6.1. Requisitos

Indo de encontro ao que foi referido anteriormente, de seguida apresentaram-se os requisitos necessários, que deverão estar presentes na arquitetura de monitorização integrada.

De uma forma geral, a plataforma de monitorização deverá contar com um conjunto de funcionalidades base que correspondem aos seguintes requisitos funcionais:

- RF1: Proporcionar uma monitorização centralizada e distribuída;
- RF2: Suportar os protolocos *SNMP*, *ICMP* e outros relacionados;
- RF3: Visualizar todos os problemas existentes na rede;
- RF4: Oferecer uma interface simples e intuitiva;
- RF5: Permitir associação de ficheiros *MIB;*
- RF6: Receber e processar *traps;*
- RF7: Indicação do estado dos equipamentos e serviços;
- RF8: Suportar a monitorização a nível aplicacional;
- RF9: Execução de comandos remotos e automáticos;
- RF10: Suportar a monitorização para a virtualização;
- RF11: Permitir a configuração e personalização das notificações;
- RF12: Evitar o envio de notificações desnecessárias e/ou duplicadas;

Terá de permitir a definição e/ou configuração de alguns aspetos específicos, à qual permitam ao gestor de redes obter uma maior personalização e flexibilidade na configuração e definição de alguns parâmetros da rede, tais como:

- RF13: Dispositivos e grupos de dispositivos;
- RF14: *Monitoring templates* para recolha e monitorização de dados;
- RF15: Itens a monitorizar e *triggers;*
- RF16: Gráficos personalizados, com possibilidade de partilha;
- RF17: Utilizadores, grupos de utilizadores e permissões respetivas;
- RF18: Dependência de equipamentos e serviços;
- RF19: Notificações para utilizadores e grupos de utilizadores;
- RF20: Notificações por correio eletrónico e outras plataformas relacionadas;
- RF21: Mapas de rede personalizados;

A plataforma de monitorização integrada terá de disponibilizar ao gestor de redes a visualização dos vários parâmetros da rede, tais como:

- RF22: Estado da rede num todo;
- RF23: Dispositivos e grupos de dispositivos;
- RF24: Monitorização dos múltiplos *sites*;

O gestor de redes terá de monitorizar, na plataforma de monitorização integrada, os vários equipamentos e serviços que constituem a sua rede entre os quais:

- RF25: Dispositivos heterógenos;
- RF26: *Software* instalado nos dispositivos monitorizados;
- RF27: Serviços e conteúdos de serviços;
- RF28: Máquinas virtuais e *LXC containers*;

Por fim, a solução integrada para a plataforma de monitorização terá de ser:

- RF29: Preferencialmente livre e *open-source;*
- RF30: Suportar alta disponibilidade;
- RF31: Fortemente escalável;

Nesta secção apresentou-se, de forma sucinta, os requisitos funcionais que terão de estar presentes na proposta da arquitetura de monitorização para a instituição Governamental. Estes foram elaborados tendo por base a análise da infraestrutura desta, como também as suas necessidades e dificuldades quando ocorre uma falha.

3.7. Conclusão

Neste capítulo discriminou-se e contextualizou-se a atual infraestrutura de rede da instituição Governamental, onde se verificou as suas características e suas limitações. Descreveu-se o caso de estudo para o presente projeto, onde se salientou a sua dimensão, nomeadamente as infraestruturas e serviços, como também se destacou aspetos únicos e pertinentes de uma organização Governamental, características estas que tornam a tarefa de monitorização complexa, mas fundamental para o funcionamento normal da instituição Governamental.

Constatou-se que, no desenrolar dos anos, os serviços sobre a rede da instituição Governamental tiveram um crescimento enorme e esperado face à evolução tecnológica, fazendo consequentemente que a sua infraestrutura se tornasse complexa e de igual modo crítica. Com a recente aquisição da sua própria rede privativa, houve uma centralização de todos os serviços da instituição e uma partilha central dos recursos a partir dos seus *datacenters*. Esta centralização veio permitir responder à demanda existente de serviços para os seus 265 *sites*, contudo trouxe um ponto crítico em caso de falha nos seus *datacenters.* A monitorização de todos os serviços e infraestruturas dos *datacenters* da instituição Governamental é deveras um dos pontos mais fundamentais para a monitorização, devido aos constrangimentos e consequências em caso de falha de um destes. Em suma, coma centralização dos serviços da instituição Governamental nos seus *datacenters*, na situação de falha destes, toda a instituição Governamental fica sem serviços.

Os *sites* possuem características distintas e próprias umas das outras de acordo com a natureza das suas funções. Esta infraestrutura pode-se considerar como sendo bastante heterogénea, constituída por múltiplas entidades de natureza e necessidades diferenciadas, dispersas geograficamente ao longo das ilhas atlânticas. Esta heterogeneidade torna complexa a implementação de sistemas de monitorização convencionais, fazendo consequentemente que a arquitetura de monitorização deva estar preparada para tamanha diversidade de dispositivos, serviços e suas particularidades e especificidades de monitorização.

A arquitetura de monitorização terá de permitir a centralização da gestão de todos os dispositivos e serviços da infraestrutura da entidade Governamental, como também permitir mecanismos de monitorização distribuídos, face às características da infraestrutura da rede privativa da instituição Governamental. Terá de ter em conta o tamanho da equipa que possui a responsabilidade na gestão e monitorização dos sistemas, sendo necessário a definição de procedimentos que auxiliem os gestores de sistemas e redes no processo de tomada de decisão.

O próximo capítulo descreverá a proposta da arquitetura de monitorização para a instituição Governamental, tendo por base os requisitos aqui definidos e especificidades mencionadas da sua natureza Governamental.

4. Proposta Arquitetural

Este capítulo sintetiza a proposta arquitetural de monitorização para a rede de grande dimensão da instituição Governamental, tendo por base a características e requisitos referenciados no capítulo anterior. Ao longo do capítulo serão aprofundados em detalhe aspetos relacionados com a forma como a arquitetura está segmentada, nomeadamente grupos, alertas e notificações, disposição da informação e fluxos de comunicação da própria arquitetura.

A arquitetura proposta suportará requisitos, previamente identificados, importantes para o funcionamento normal da instituição Governamental, para auxílio dos seus gestores de sistemas e redes na tomada de decisão. No caso da escalabilidade será necessário assegurar o fácil crescimento da arquitetura de monitorização e disposição clara de toda informação em tempo real. Suportará uma componente forte resiliente a falhas, principalmente nas infraestruturas dos *datacenters* da instituição Governamental face à sua criticidade. A segmentação dos dispositivos / serviços por grupos é um dos principais pontos fundamentais para a instituição Governamental para a célere busca e visualização da informação pretendida. Os grupos definidos tiveram por base o tipo de dispositivos, serviços e localização, permitindo assim uma fácil identificação e busca de dispositivos e/ou serviços por site da instituição Governamental.

A recolha dos dados de monitorização terá por base os protocolos de monitorização baseada em gestor-agente e protocolos convencionais de monitorização como por exemplo *SNMP (Simple Network Management Protocol).* Os protocolos utilizados suportarão a monitorização de mais baixo nível, como é o caso do *hardware*, e a monitorização aplicacional. Devido à criticidade e sensibilidade da informação, mecanismos de segurança para encriptação dos dados de monitorização são necessários, implementando assim mecanismos de segurança que garantam a confidencialidade dos dados de monitorização de toda a rede da instituição Governamental.

De seguida, as próximas secções irão detalhar os vários pontos constituintes da proposta arquitetural, nomeadamente a sua arquitetura geral (4.1), a forma como é efetuada a comunicação entre *proxys* e servidor (4.1.1), como é assegurada a segurança da informação crítica entre estes, a segmentação dos grupos baseada em tipos de dispositivos e/ou tipos de serviços (4.2), e o tipo de informação disponibilizada para auxílio de tomada de decisões aos gestores de sistemas e redes da instituição Governamental (4.2.1).

4.1. Proposta de Arquitetura de Monitorização

Tendo por base o referido anteriormente, efetuou-se o planeamento da arquitetura de monitorização. A arquitetura terá de suportar a monitorização dos diversos serviços e dispositivos heterogéneos de toda a infraestrutura da instituição Governamental, incluindo os seus *datacenters*, garantindo uma monitorização robusta e fiável independentemente das diferentes naturezas e especificidades que cada *site* da instituição Governamental possui.

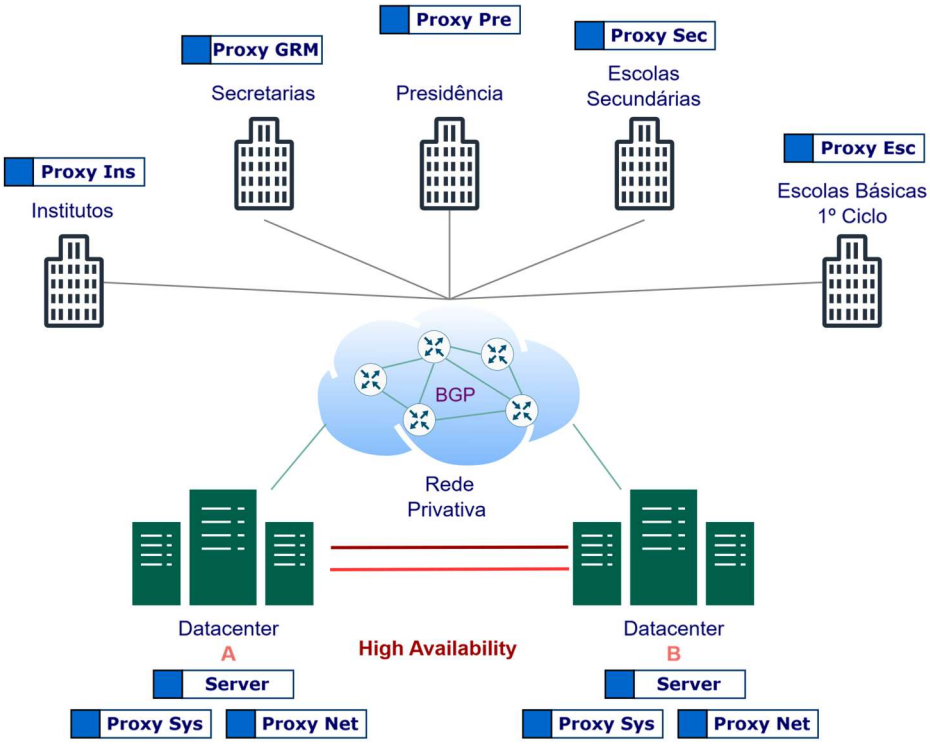

Figura 4.1: Arquitetura geral para monitorização da instituição Governamental.

Na *Figura 4.1* tem-se representado a arquitetura geral para a monitorização de toda a infraestrutura e serviços incluindo os seus *datacenters* da instituição Governamental. A arquitetura é constituída pelo servidor central, a qual terá a cargo o armazenamento e análise de toda a informação obtida pelos *proxys,* e pelos próprios *proxys* presentes em cada *site* da instituição Governamental.

Face à necessidade de garantir uma forte resiliência a falhas na sua infraestrutura mais crítica da instituição Governamental, a monitorização dos seus *datacenters* é assegurada por dois *proxys* distintos, o de sistemas (*Proxy Sys*) e o de redes (*Proxy Net*), em regime de alta disponibilidade. Ambos os *proxys* possuem funções de monitorização distintas, sendo que o de sistemas possui características direcionadas para a monitorização de sistemas tais como servidores, *storage* e camada aplicacional, enquanto o de redes possui características direcionadas para *switches*, *routers* e *acess points*. Esta segmentação de monitorização nos *datacenters* da instituição

Governamental permitirá a utilização dos recursos das máquinas de *proxys* mais eficientemente. De igual modo, o servidor central está em regime de alta disponibilidade, garantindo assim a contínua monitorização mesmo em cenários de falha de um dos *datacenters* da instituição Governamental.

Os *proxys* permitirão a implementação de uma monitorização distribuída que, por sua vez, terá a cargo a recolha das métricas e, porventura, envio ao servidor central. Estes serão instalados nos *sites* pertencentes à rede privativa da instituição Governamental, onde irão monitorizar, na infraestrutura do respetivo local, métricas tais como *uptime* dos dispositivos, dispositivos *offline*, latência, retransmissão de pacotes, perda de pacotes, parâmetros estes que permitirão obter-se uma visão geral sobre a qualidade da infraestrutura de rede dos *sites* da instituição Governamental. A nomenclatura para cada *proxy* tem por base o tipo de *site*, nomeadamente se é uma secretaria, instituto, escola básica ou secundária e o *ID* único do *site* da instituição Governamental. Cada *site* possui um *ID* único onde será utilizado também para juntar ao tipo de *proxy* que irão existir. Abaixo fica a nomenclatura de base para os *proxys* que ficarão nos 265 sites da instituição Governamental:

- ***Proxy Inst-043*** – *Proxy* de um *site* categorizado como Instituto com o *ID* único 043.
- ***Proxy Grm-001*** – *Proxy* de um *site* categorizado como Secretaria com o *ID* único 001.
- ***Proxy Esc-057*** – *Proxy* de um *site* categorizado como Escola Básica com o *ID* único 057.
- ***Proxy Sec-002*** – *Proxy* de um *site* categorizado como Escola Secundária com o *ID* único 002.
- ***Proxy Con*-094** – *Proxy* de um *site* categorizado como Conservatória com *ID* único 094.
- ***Proxy Pre-012*** – *Proxy* de um *site* categorizado como Presidência com o *ID* único 012.

O servidor central irá receber, de inúmeros *proxys*, as métricas recolhidas a partir dos *sites* que constituem a rede privativa da instituição Governamental e efetuar a análise das mesmas com base nos valores esperados e/ou definidos. Numa situação anómala, irá emitir uma notificação, nos meios definidos, para os gestores de sistemas e redes, sobre a situação detetada. De maneira a garantir a robustez, fiabilidade e integridade da arquitetura foi também delineado que as comunicações entre os *proxys* e o servidor, utilizarão protocolos de encriptação dando assim uma maior segurança na troca da informação entre estes.

4.1.1. Comunicação entre *Proxys* e Servidor

A encriptação das comunicações entre *proxys* e servidor é obtida com recurso a utilização de *PSK (Pre Shared Key*), onde são utilizadas chaves *random* com comprimento máximo de *256-byte*. Este método irá garantir que todo o tráfego, incluindo as métricas recolhidas pelos *proxys* e os ficheiros de configuração dos equipamentos que são enviados a partir do servidor, toda essa comunicação e informação está devidamente encriptada, aumentando assim os níveis de segurança da arquitetura proposta.

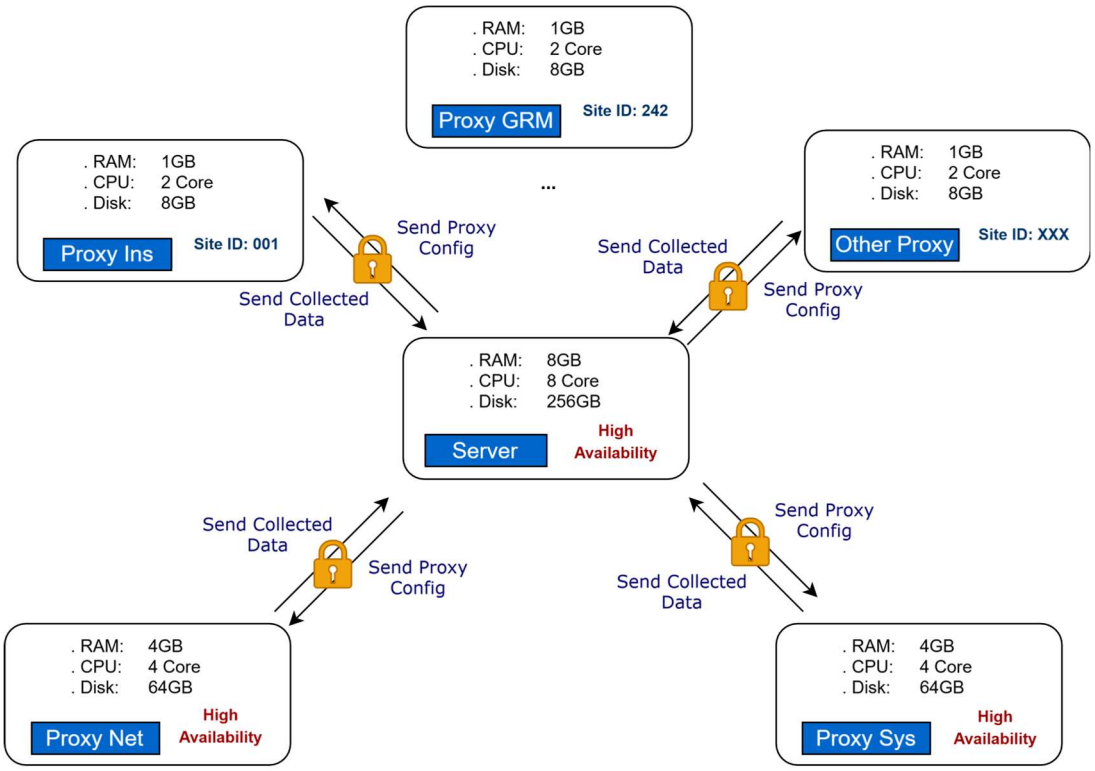

Figura 4.2: Arquitetura de comunicação entre *proxys* e servidor.

A *Figura 4.2* representa detalhadamente como a comunicação é efetuada entre o servidor e os *proxys.* Os *proxys,* que estarão ao longo dos 265 *sites* da instituição Governamental, irão enviar todas as métricas obtidas e receber instruções a partir do servidor, onde todo este fluxo de comunicação irá estar encriptado, garantindo assim a confidencialidade dos dados de monitorização de toda a instituição Governamental.

Os *proxys* terão a capacidade de, em caso de perda de comunicação com o servidor, continuamente efetuar a monitorização das métricas e armazená-las internamente, para que quando for restabelecido a comunicação com o servidor, lhe reenviar. Este modo permitirá oferecer uma maior resiliência à arquitetura proposta, garantindo a integridade dos dados de monitorização mesmo no cenário de quebra de comunicação com o servidor.

4.1.2. Comunicação entre *Proxy* e Dispositivos

O processo de recolha das métricas de monitorização de cada *proxy* utilizará sempre que possível, o modelo gestor-agente assim como os protocolos de monitorização tradicionais como o *SNMP (Simple Network Management Protocol).* Devido à centralização dos seus serviços nos seus *datacenters*, a maior parte da infraestrutura existente nos *sites* da instituição Governamental é constituída por equipamentos de rede, tais como *routers*, *switches* e *access points,* e equipamentos tais como impressoras e computadores.

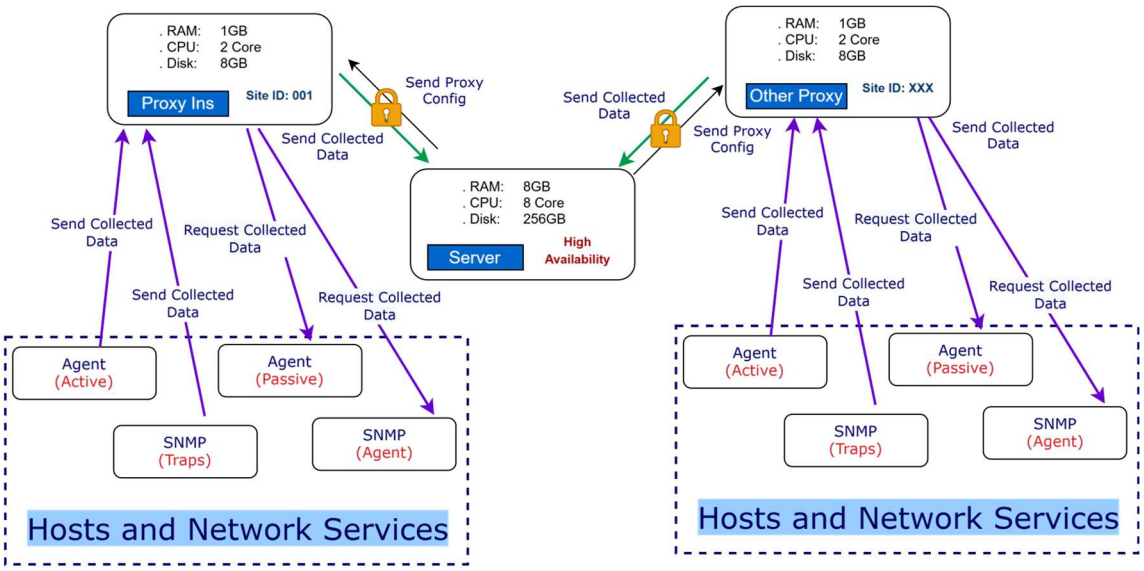

Figura 4.3: Arquitetura de comunicação monitorização entre *proxys* e dispositivos.

A *Figura 4.3* mostra o fluxo de comunicação de cada *proxy* desde os dispositivos e/ou serviços que está a monitorizar até ao servidor. Podemos constatar a roxo o fluxo da monitorização por parte do *proxy* aos dispositivos e/ou serviços existentes no referido *site*, e a verde o envio de todo esses dados para o servidor. Esta segmentação de fluxo de comunicações entre *proxys*, servidor e dispositivos e/ou serviços a monitorizar é um dos pontos principais para proposta de arquitetura distribuída ser fortemente escalável. Esta separação permite o não afunilamento dos meios de comunicação normal de monitorização dos dispositivos com o servidor, ficando este a cargo na totalidade dos *proxys*.

A escalabilidade na arquitetura proposta é assegurada através desta separação e definição dos fluxos de comunicação entre dispositivos e servidor, permitindo assim também uma melhor e eficaz utilização dos recursos do servidor para a analítica dos dados obtidos a partir dos diversos *proxys* existentes na instituição Governamental.

4.2. Estrutura da Informação

A estrutura da informação definida tem uma estrutura *top down* lógica e coerente de maneira auxiliar os gestores de sistemas e redes no processo de tomada de decisão. Deste modo, foi elaborada uma organização da informação da monitorização, a qual tem por base três principais parâmetros nomeadamente:

- ***Site*** – *ID* único de cada *site* da instituição Governamental;
  - Dispositivos como *switches*, *routers*, impressoras e *access points* presentes em cada *site*.

- **Sistemas** – Dispositivos e/ou serviços geridos pela equipa de sistemas;
  - Dispositivos como *hipervisors*, servidores, armazenamento passando desde a camada de *hardware* até à aplicacional.

- ***Datacenter*** - Dispositivos e/ou serviços com a gestão da equipa de redes;
  - Dispositivos como *switches*, equipamentos e ligações de *ISP*, *routers* e *firewalls*.

A separação por site permitirá não só a fácil filtragem de dados de monitorização, como também a criação de grupos de utilizadores e notificações por *site,* segmentando também a responsabilidade de intervenção por locais.

Os parâmetros distintos de sistemas e *datacenters*, permitirão de igual modo dividir a responsabilidade de intervenção e gestão dos dispositivos pelas equipas existentes da instituição Governamental. De igual modo a filtragem de informação mais lógica é repartida consoante o tipo de dispositivo e/ou serviço, tornando assim o processo de obtenção de informação mais eficiente.

4.2.1. Visualização da Informação

A visualização da informação terá de possuir dados agregados de todos os *sites* da instituição Governamental, contendo informação relevante que demostre, em tempo real, o seu atual estado. Terá de conter informação clara e pertinente, onde todos os serviços considerados críticos para o funcionamento da instituição Governamental, terão de ser facilmente interpretados, para uma maior celeridade na identificação da causa da anomalia.

A informação referente aos *datacenters* da instituição Governamental terá de permitir aos gestores de sistemas e redes a visualização geral do seu funcionamento, através de dados agregados, como também ajudar no processo de tomada de decisão, nomeadamente na análise dos limites dos recursos atuais dos *datacenters*. Este último pormenor irá fazer com que a instituição Governamental possa antecipar necessidade de renovação e/ou aquisição de mais recursos tendo por base a monitorização dos seus *datacenters*.

4.3. Conclusão

Este capítulo apresentou e discriminou a proposta de uma arquitetura de monitorização distribuída para a instituição Governamental, tendo por base a análise efetuada no capítulo anterior. A arquitetura proposta teve como base a necessidade de uma arquitetura resiliente a falhas, fortemente escalável, que auxilie os gestores de sistemas e redes no processo de tomada de decisão quando uma anomalia é detetada. A presente proposta teve em consideração mecanismos resilientes a falhas inclusive nos *datacenters* da instituição Governamental, face à sua criticidade na disponibilização de serviços para os seus 265 *sites*. O servidor e os *proxys* dos *datacenters* estão em regime de alta disponibilidade, garantindo assim a integridade dos dados de monitorização da instituição Governamental, mesmo num cenário de falha total de um dos seus *datacenters*. A segmentação da monitorização dos dispositivos e/ou serviços nos *datacenters* da instituição Governamental através de dois *proxys* distintos tem como finalidade uma melhor eficácia no fluxo de dados de monitorização e recursos computacionais dos *proxys* com base no tipo de monitorização.

A nomenclatura para os *proxys* teve por base a categorização dos *sites* da instituição Governamental, onde utilizou-se essa categorização junto com o *ID* único de cada *site*. A arquitetura proposta definiu também os fluxos de comunicação entre *proxys* e servidor, onde, devido ao tipo de informação sensível que passa na instituição, foram definidos protocolos que garantam a encriptação de todos os dados de monitorização da instituição Governamental garantindo assim a sua confidencialidade. De igual modo foi também estabelecido o fluxo de comunicação da monitorização dos *sites* da instituição Governamental desde o *proxy* ao servidor, onde será utilizado sempre que possível o modelo gestor-agente e, por fim, os protocolos convencionais de monitorização como é o caso do *SNMP (Simple Network Management Protocol).*

A nível da estrutura da informação foram definidos três parâmetros de base nomeadamente *sites*, sistemas e redes. Estes parâmetros irão permitir o agrupamento da informação por local, por tipo de dispositivo e/ou serviço, permitindo uma eficaz divisão da responsabilidade de intervenção, por locais ou equipas. Esta segmentação será benéfica no envio de notificações de forma mais eficiente às equipas com a responsabilidade na gestão das áreas em concreto. A visualização da monitorização da instituição Governamental terá de possuir dados agregados, dos seus *sites* e *datacenters*, que auxiliem os gestores de sistemas e redes no processo de tomada de decisão, não só aquando de uma anomalia como também na gestão dos recursos dos *datacenters* da instituição Governamental.

O próximo capítulo descreverá a implementação da arquitetura de monitorização para a instituição Governamental, tendo por base a proposta arquitetural definida neste capítulo.

5. Implementação

Este capítulo pretende detalhar o processo de implementação da proposta arquitetural de monitorização distribuída para a instituição Governamental, referenciada no capítulo anterior, na sua infraestrutura de *datacenters* e respetivos *sites*. Numa primeira fase será necessário efetuar uma pesquisa e seleção de *software open-source*, a serem equacionados como plataforma de monitorização, de acordo com os requisitos definidos na arquitetura e monitorização da instituição Governamental.

Os *datacenters* são considerados a infraestrutura mais crítica da instituição Governamental, face à centralização dos serviços de todos os 265 *sites* nestas infraestruturas. Deste modo, a monitorização dos *datacenters* foi definida como a primeira prioridade na implementação da arquitetura de monitorização distribuída. Esta prioridade fez com que fosse necessário efetuar um procedimento de monitorização para diferentes tipos de equipamentos que compõem o *datacenter* da instituição Governamental. Esta definição de procedimentos é fundamental na garantia da padronização de monitorização de dispositivos e/ou serviços ao longo de toda a infraestrutura da instituição.

Será necessário garantir a segmentação de toda a informação obtida, fazendo-a com a criação de grupos tendo por base os três parâmetros referenciados no capítulo anterior, isto é, *sites*, sistemas e redes. Ao longo da implementação foi necessário efetuar-se reajustes aos *templates* de monitorização de acordo com as orientações fornecidas pelas equipas de gestores da entidade Governamental. Estes reajustes são importantes para a garantia de uma monitorização fiável e fidedigna aos seus gestores de sistemas e redes, para que quando receberem um alerta e/ou notificação, se possa garantir que é realmente uma situação importante e não uma situação meramente informacional sem qualquer tipo de impacto para a instituição Governamental.

Os sistemas de notificação / alerta terão de suportar diversos tipos de media, assegurando o envio das notificações para grupos de utilizadores e para os sistemas de visualização da infraestrutura de monitorização da instituição Governamental. A disposição da informação será efetuada com recurso a *dashboards* dinâmicos, onde a informação é atualizada em tempo real, dando enfâse a dispositivos e/ou serviços críticos para o funcionamento normal da instituição.

As próximas secções irão sintetizar a pesquisa e seleção do *software* de monitorização para a proposta da arquitetura de monitorização (5.1), a implementação da plataforma de monitorização (5.2) a qual englobará os seus *datacenters*, *sites* remotos, estrutura de informação, *templates* criados e, por fim, expor como que todos os dados de monitorização estão representados graficamente (5.3).

5.1. Pesquisa e Seleção Plataforma Monitorização

Após a definição dos requisitos para a arquitetura de monitorização distribuída, efetuou-se uma comparação e análise das plataformas de monitorização *open-source* atualmente existentes, tendo se restringido esta análise às plataformas *Prometheus, Naggios Core, Grafana, Zabbix* e *Icinga*. Neste subcapítulo irá constar a comparação entre as ferramentas de monitorização integradas, quais os critérios usados na avaliação de ambas, definidos em reunião com os responsáveis pela gestão e monitorização da instituição Governamental.

Efetuou-se uma pesquisa da documentação oficial sobre cada uma destas plataformas *open-source* e verificou-se que todas estas possuem pontos fortes, distintos umas das outras. No caso do *Prometheus*[1] verificou-se que é uma ferramenta bastante completa, possuindo mecanismos de autodescoberta na rede, possuindo a possibilidade de criação de *templates* específicos para determinados *hosts* e/ou serviços.

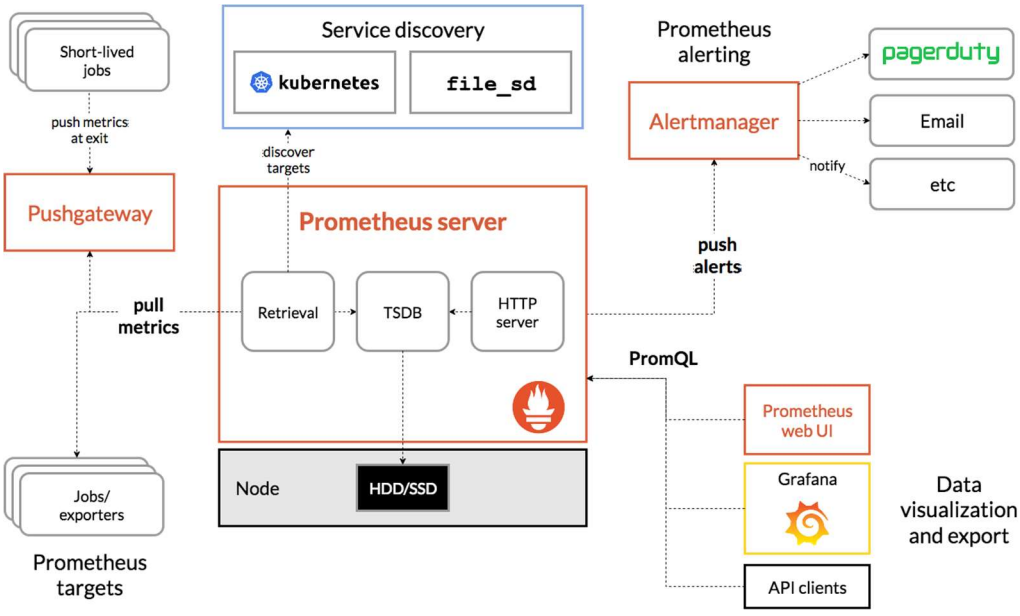

Figura 5.1: Arquitetura geral da plataforma monitorização *Prometheus,* retirado de [42].

A *Figura 5.1* mostra a arquitetura geral da plataforma *Prometheus*, retirada da sua documentação oficial, onde podemos verificar que esta utiliza para visualização dos dados de monitorização a ferramenta *Grafana*. O *Prometheus* possui a capacidade de ser configurado para a alta disponibilidade, tal como representado na *Figura 5.2*, cumprindo deste modo, um dos requisitos delineados na proposta de arquitetura de monitorização.

[1] https://prometheus.io/

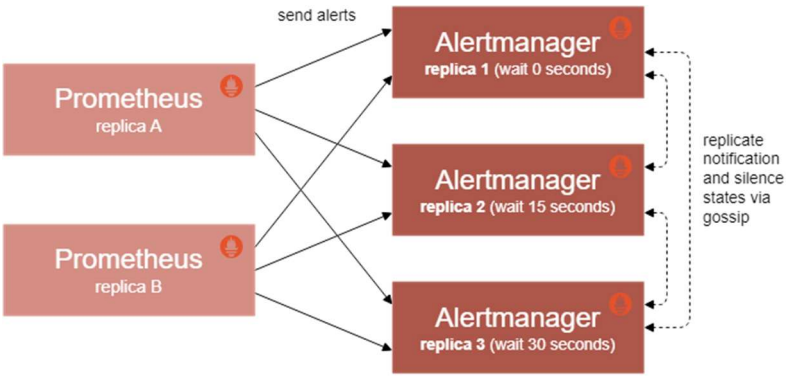

Figura 5.2: Arquitetura para alta disponibilidade da plataforma *Prometheus,* retirado de [42].

A plataforma de monitorização *Nagios Core*[2] é das mais maduras *open-source* atualmente existentes, face à sua longevidade. Esta tem suporte para vários *plugins* para efetuar a recolha de métricas de monitorização, de vários tipos de *hosts* e/ou serviços. Não possui qualquer tipo de dependência na sua arquitetura de outros *softwares* para o seu funcionamento. A visualização dos dados é através da sua própria interface gráfica, permitindo a total personalização dos dados de monitorização.

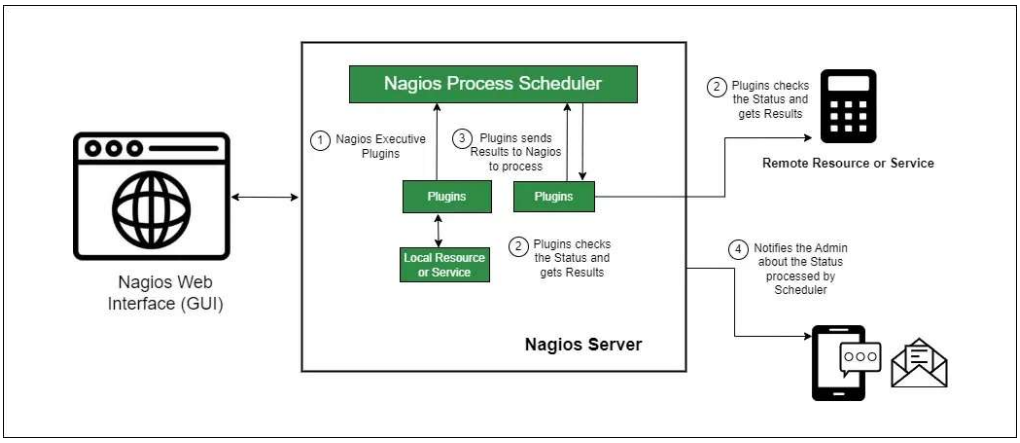

Figura 5.3: Arquitetura geral da plataforma monitorização *Nagios Core,* retirado de [43].

O Nagios Core [43] possui a possibilidade da utilização do seu próprio agente em máquinas *Linux*, fazendo com que seja possível centralmente pela plataforma, configurar ações automáticas com base em eventos.

O Grafana[3] é uma ferramenta que ajuda na visualização dos dados obtidas de forma rápida e intuitiva. Tem como grande vantagem a utilização de *dashboard* pré configurados para tipos de *hosts* e/ou serviços. A *Figura 5.4* mostra um exemplo de um *dashboard* base para servidores *web*.

[2] https://www.nagios.org/
[3] https://grafana.com/

Figura 5.4: Exemplo de um *dashboard* da plataforma *Grafana*.

Apesar da plataforma *Grafana* destacar-se a nível da representação dos dados obtidos, esta simplesmente efetua um tratamento da informação com base na recolha dos dados a partir de uma outra plataforma. A recolha das métricas de monitorização terá de ser efetuada por uma outra plataforma para que o *Grafana* possa se integrar, e efetuar o tratamento desses mesmos dados, para grafismos pré configurados.

O *Zabbix*[4] é uma plataforma de monitorização polivalente, a qual possui a integração com imensas marcas e serviços. Tal como o *Nagios Core,* este possui o seu próprio agente tanto para *Windows* como para *Linux*, fazendo com que seja possível obter-se métricas de monitorização mais precisas e despoletar ações de forma automática.

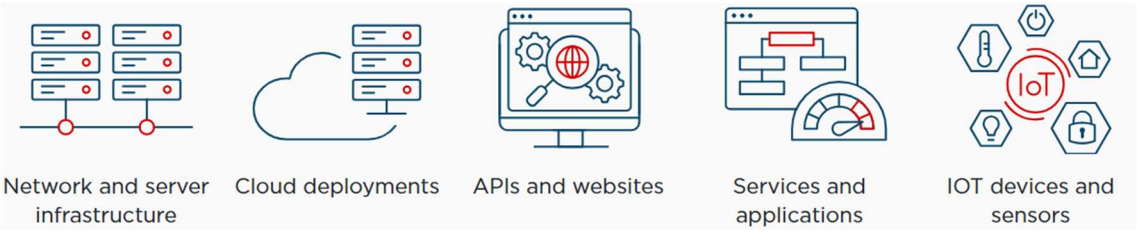

Figura 5.5: Vertentes de monitorização da plataforma *Zabbix*.

Esta possui capacidades de alta disponibilidade e está preparada nativamente para monitorização distribuída, com a utilização de *proxys* na sua configuração. Possui capacidade de criação de modelos de monitorização específicos para *hosts* e/ou serviços, tornando desta forma a monitorização diversificada consoante as necessidades de monitorização.

[4] https://www.zabbix.com/

O *Icinga* é uma plataforma de monitorização relativamente recente, em que sua origem advém de um *fork* a partir do *Nagios Core*. Tem como grandes características o suporte para alta disponibilidade, agente próprio e sistema de interface gráfica interno e personalizável, para disposição dos dados de monitorização entre outros mais.

Após reunião com os responsáveis pela gestão e monitorização da instituição Governamental, ficou estabelecido que a plataforma de monitorização seria decidida entre *Nagios Core* e *Zabbix*. Para tal, com base nos requisitos estabelecidos, foram definidos os requisitos prioritários. Foi a partir destes, que foi efetuada a comparação entre as duas plataformas, de maneira a chegar-se a uma tomada de decisão.

Numa primeira fase recolheu-se, a partir da documentação oficial de cada uma das plataformas, as características e funcionalidades das mesmas sendo que, na grande maioria destas, ambas possuem as mesmas características. Após este levantamento, com base nos requisitos definidos para a proposta arquitetural, realizou-se uma análise sobre todos estes requisitos são cobertos, com base nas características e funcionalidades de cada uma das plataformas referidas.

A *Tabela 1* representa um quadro resumo dos requisitos considerados mais importantes / prioritários, definidos em reuniões com os responsáveis pela monitorização e gestão da instituição Governamental, para a seleção da plataforma de monitorização que melhor se enquadra nos requisitos definidos na proposta arquitetural, onde verifica-se se são cumpridos nas plataformas descritas.

	Nagios Core	*Zabbix*
RF1 - Monitorização centralizada e distribuída	✓	✓
RF3 - Visualizar todos os problemas	✓	✓
RF4 - Interface simples e intituitiva	✓	✓
RF5 - Associação ficheiros MIB	✓	✓
RF14 - Templates para recolha de dados	×	✓
RF18 - Dependência de equipamento e serviços	✓	✓
RF20 - Notificações por email e outros	✓	✓
RF21 - Mapas Personalizados	✓	✓
RF24 - Multiplos Sites	✓	✓
RF29 - Open-source	×	✓

Tabela 1: Análise das plataformas em relação aos requisitos prioritários.

Após a análise, verificou-se que dois dos requisitos considerados prioritários não têm o devido suporte, na plataforma *Nagios Core*, pois esta não possui facilidade na criação e importação de *templates* de monitorização ao invés da plataforma *Zabbix*. A plataforma de monitorização *Nagios Core* possui capacidade de implementação de monitorização distribuída, contudo é necessário a aquisição de licenças pagas, não cumprindo o requisito de uma plataforma totalmente *open-source*. Face a um dos principais fatores da infraestrutura da instituição Governamental ser a enorme diversidade de equipamentos e serviços heterogéneos, em reunião com os responsáveis pela gestão e monitorização da instituição Governamental, foi decidido adotar a implementação da plataforma de monitorização *Zabbix*.

5.1.1. Plataforma *Zabbix*

Será utilizado por base o relatório da Licenciatura em Engenharia Informática [44], onde foram atualizados alguns pontos de acordo com a evolução da plataforma, onde todas as imagens utilizadas são documentação da plataforma *Zabbix*.

O *Zabbix* é uma plataforma de monitorização *open-source* que efetua a monitorização de inúmeros parâmetros de uma rede desde servidores, máquinas virtuais e equipamentos de rede. A sua monitorização é efetuada através de alguns protocolos específicos da plataforma, como de outros mais conhecidos para a monitorização de dispositivos em rede.

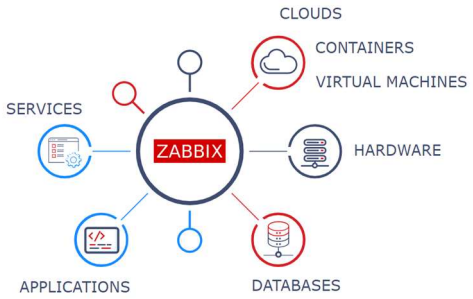

Figura 5.6: Competências da plataforma de monitorização *Zabbix*.

5.1.1.1. Arquitetura

A sua arquitetura conjuga vários elementos para a monitorização de uma rede, tais como um servidor, uma base de dados, um *web interface*, vários *proxys* e, por fim, agentes e/ou protocolos de monitorização convencionais, onde todos estes estão interligados e sincronizados para o envio e receção das métricas obtidas de dispositivos e/ou serviços na rede.

Zabbix Server

O *Zabbix server* é o ponto central de processamento de todas as métricas recolhidas na rede. Este possui a função de pedir, receber e armazenar todos os dados obtidos. É na análise destes dados que pode despertar um *trigger*, ou seja, uma ação que pode ser desde o envio de um simples *email* a uma ação automática como reiniciar um serviço.

É também através do *Zabbix server* que existe uma interação com *Zabbix proxy* e agentes, que também podem originar *triggers* tal como referido anteriormente.

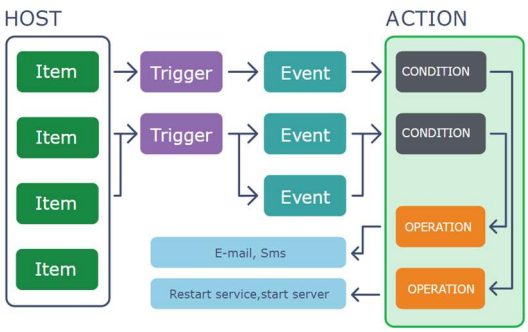

Figura 5.7: Fluxo de geração de uma ação com base na análise do *Zabbix server*.

Zabbix Proxy

O *Zabbix proxy* à semelhança do *Zabbix server*, efetua a recolha de informação dos dispositivos na rede, onde os pedidos são feitos e processados no *Zabbix proxy*. Isto permite efetuar uma distribuição de carga entre o *Zabbix proxy* e *Zabbix server*, onde os equipamentos que estão a ser monitorizados através do *proxy*, os seus dados recolhidos são armazenados temporariamente neste, onde por sua vez é enviado para o *Zabbix server*.

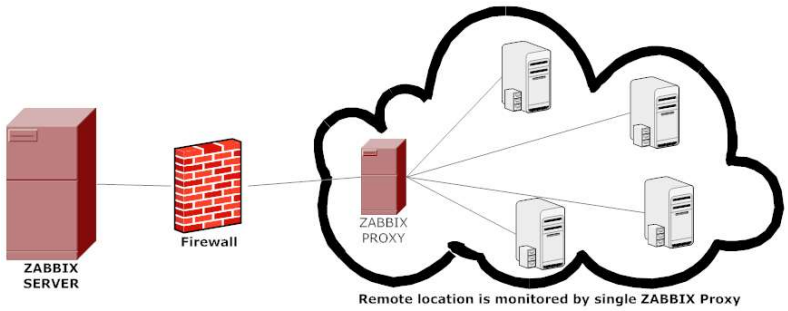

Figura 5.8: Arquitetura de monitorização com utilização de *proxys*.

Agente *Zabbix*

Zabbix agent é um tipo de processo para monitorização de um *host* próprio da plataforma *Zabbix*. Este é diretamente instalado no *host*, onde irá proceder à recolha dos dados localmente para posterior envio ao *Zabbix server ou Zabbix proxy,* a fim de estes analisarem os mesmos. *Zabbix agent* é um mecanismo extremamente eficiente na recolha de dados do *host*, devido ao seu uso de '*native system calls*' na recolha de informação.

A plataforma *Zabbix* estruturou o *Zabbix agent* em dois modos: passivo e ativo. A principal diferença entre estes dois tipos de agente está na forma como estes comunicam as métricas entre o *Zabbix server* ou *Zabbix proxy*, sendo que ambas devem ser utilizadas para casos distintos.

O **agente *Zabbix* no modo passivo** as métricas recolhidas são obtidas pelo *server* ou *proxy* ao *Zabbix agent*. O *server ou proxy* comporta-se como um *poller,* utilizando o protocolo TCP na porta 10050, efetuando pedidos ao *Zabbix agent* de dados como podemos verificar na *Figura 5.9*. A vantagem deste tipo de abordagem é a isenção na parte do *host* de qualquer processamento de dados ficando este somente de corresponder aos dados solicitados pelo *Zabbix server* ou *Zabbix proxy*.

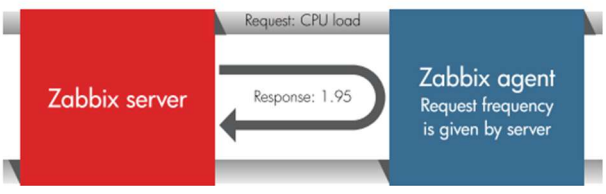

Figura 5.9: Agente *Zabbix* no modo passivo.

O **agente *Zabbix* no modo ativo,** a forma como são obtidas as métricas do *host* é diferente aquando do modo passivo. Neste, o *Zabbix agent* efetua o pedido ao *Zabbix server* ou *Zabbix proxy*, acerca que parâmetro é para ser transmitido, e com base na resposta, o agente envia o respetivo valor como podemos verificar na *Figura 5.10*. A grande vantagem deste tipo de abordagem incide no fato de o processamento estar do lado do agente, reduzindo, por sua vez, a carga no *Zabbix server*.

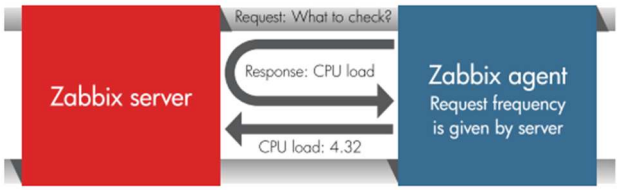

Figura 5.10: Agente *Zabbix* no modo ativo.

5.1.1.2. *Templates*

A plataforma de monitorização *Zabbix* possui inúmeros *templates* base para várias situações e equipamentos a monitorizar na rede. Um *template* é um conjunto de condições associados a itens, *triggers*, gráficos, aplicações, ecrãs, *discovery rules* e *web scenarios* que, num todo, efetuam a monitorização de um *host* ou outro serviço. A escolha do *template* deverá ser feita tendo em conta a finalidade do que se pretende monitorizar e quais os componentes que o *host* possui (*hardware* e *software*). Deste modo, todos os *hosts* e/ou serviços terão de estar associados obrigatoriamente a um *template* para respetiva monitorização.

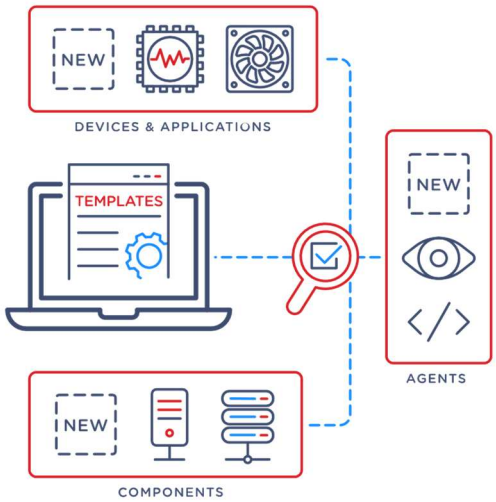

Figura 5.11: Vertentes que os *templates* possuem na plataforma monitorização *Zabbix*.

A criação de raiz de *templates* específicos é possível para dispositivos ou serviços, trazendo uma maior configuração, rigor e personalização no tipo de dados recolhidos, sendo também possível a importação de *templates* através do formato *XML*.

É possível associar *templates* a outros *templates* já criados, como demostrado na *Figura 5.12*. Isto traz como vantagem, caso seja necessário, a alteração de parâmetros do *template* em massa, fazendo com que todos os *hosts* associados a esse *template* automaticamente possua a respetiva alteração.

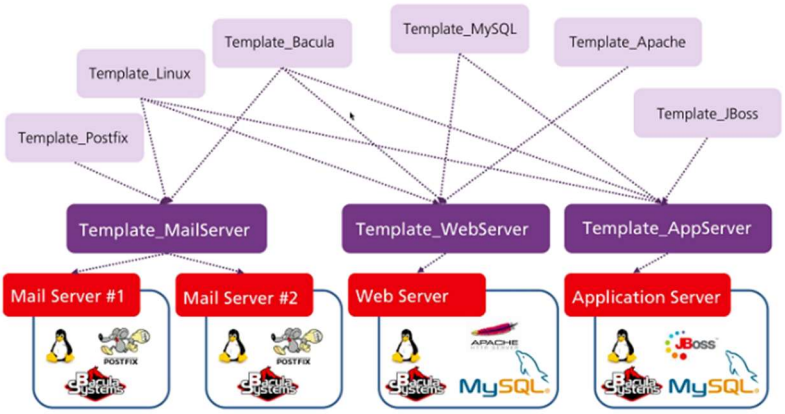

Figura 5.12: Associação de *templates* na plataforma monitorização *Zabbix*.

5.1.1.3. Notificações e Alertas

O envio de alertas gerados para os respetivos responsáveis é uma das funções mais críticas na monitorização duma rede. A plataforma *Zabbix* possuí esta característica fazendo com que seja possível informar e atuar em situações mais críticas. As notificações / alertas podem ser enviadas para utilizadores *Zabbix* como também para grupos de utilizadores em específico, permitindo assim o escalonamento dos alertas dentro da instituição.

O envio de uma notificação poderá ser feito através de diferentes canais de comunicação desde um simples *email* a um *SMS* entre outros. Uma notificação é essencialmente uma sequência de eventos originados ao longo da plataforma *Zabbix*, onde na sua origem está associada um *trigger* de um determinado *host*.

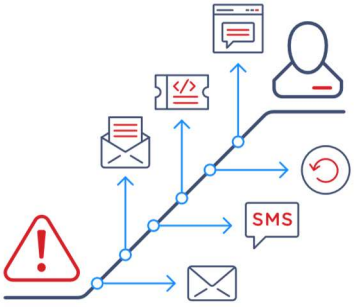

Figura 5.13: Escalonamento do envio de notificação / alerta.

5.1.1.4. Visualização Gráfica

A monitorização é efetuada através duma interface *web*, onde é possível visualizar toda a infraestrutura de rede com os respetivos *hosts* e seus parâmetros associados em tempo real. É através da monitorização da interface *web* que é possível verificar, por ordem cronológica, os valores obtidos dos vários *hosts* ao longo do tempo, sendo que esta ficará armazenada até um máximo de 2 anos por defeito.

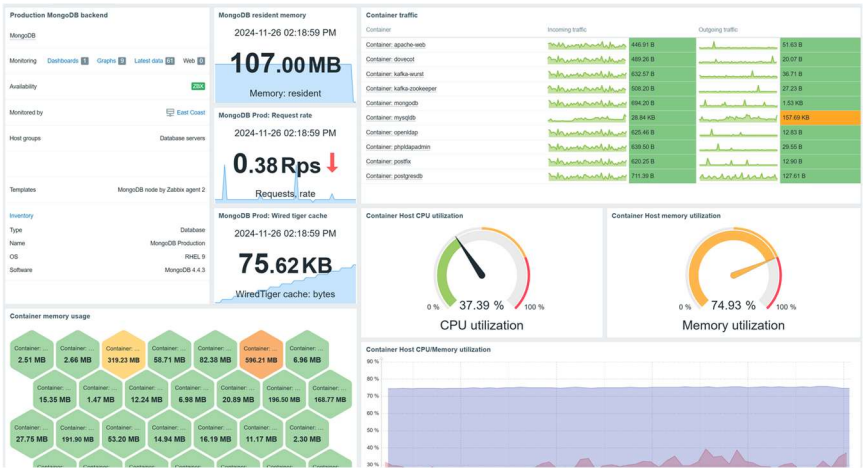

Figura 5.14: Exemplo de *dashboard* na *web interface* da plataforma *Zabbix*.

Para uma monitorização mais personalizada, a plataforma *Zabbix* permite a criação de *dashboards* pelo utilizador. Possui a característica de poder cloná-los para a monitorização de vários pontos da rede, desde *hosts,* dispositivos de rede, serviços aplicacionais entre outros, servindo de base para outros *dashboards*. Na *Figura 5.14* está representado dados agregados de um *cluster*.

Além da monitorização e métricas dos *hosts*, é através da *web interface* que permite visualizar um quadro resumo da rede monitorizada, os relatórios gerados, verificar e alterar as configurações implementadas quer nos *hosts* quer no *Zabbix.*

De seguida, ir-se-á passar para a fase de implementação da plataforma *Zabbix* na instituição Governamental.

5.2. Configuração da Plataforma

O início da implementação da plataforma de monitorização para a instituição Governamental, começou pela análise da quantidade de métricas que esta iria monitorizar. Esta análise é fundamental para a atribuição dos recursos corretos tanto para o servidor como para os *proxys*. Efetuou-se uma análise da documentação oficial da plataforma de monitorização *Zabbix* e, para o âmbito da monitorização da instituição Governamental, delineou-se a utilização de uma instalação considerada de grande dimensão, por parte da documentação oficial do *Zabbix*. Estimou-se que após a monitorização de toda a infraestrutura e serviços, esta rondaria cerca das 90 mil métricas. A *Tabela 2* mostra um excerto da documentação oficial da plataforma *Zabbix*, que demonstra os requisitos que o sistema deverá possuir em prol das quantidades de métricas de monitorização.

Tamanho da Instalação	**Métricas de Monitorização**	**CPU/vCPU *cores***	**Memória *(GiB)***
Pequeno	1 000	2	8
Médio	10 000	4	16
Grande	100 000	16	64
Muito Grande	1 000 000	32	96

Tabela 2: Requisitos de sistema para plataforma monitorização *Zabbix*.

O servidor *Zabbix* foi instalado utilizando o sistema de virtualização *Proxmox*, num *LXC container Debian 11 Bulleye*. Foi utilizado um servidor dedicado para o efeito, com cerca de 20 cores e 32GB de RAM. Para o *LXC Container* que irá conter o *Zabbix server*, foi atribuído cerca de 16 cores e 16GB de RAM, onde foi tido em conta a tabela de requisitos disponível na plataforma *Zabbix*. Estas características para o servidor *Zabbix* permitem a recolha e análise de cem mil métricas por segundo. A opção da virtualização da própria infraestrutura de monitorização, prende-se com o fato de a instituição não ficar "presa" ao servidor físico onde a aplicação irá ficar alojada, permitindo assim de uma forma fácil migrar a parte virtual não só entre servidores que possuem virtualização, como também entre *datacenters* da própria instituição Governamental.

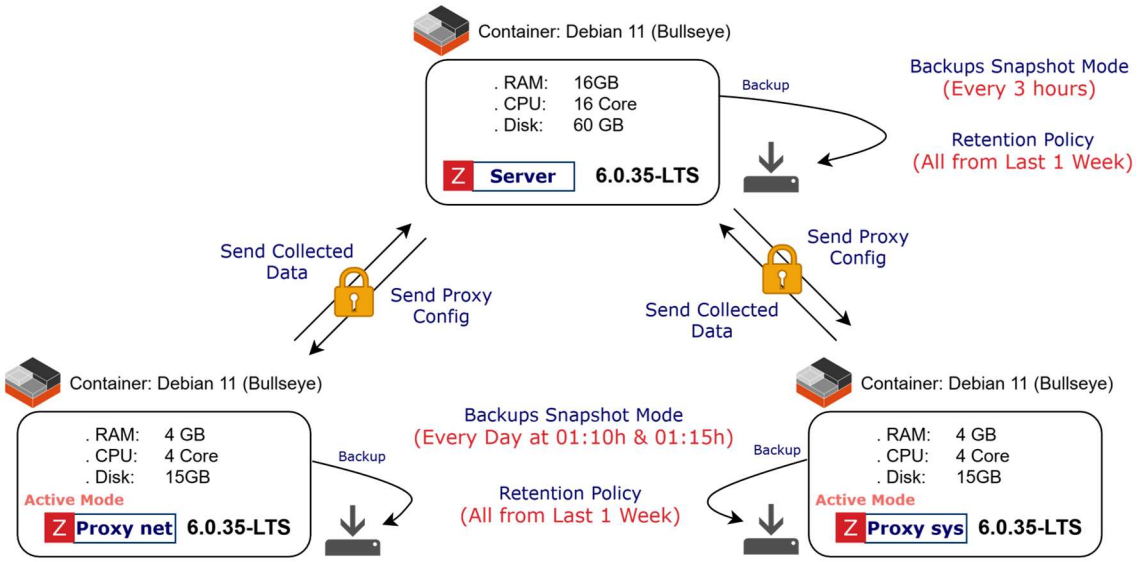

Figura 5.15: Arquitetura de monitorização servidor *Zabbix*.

A *Figura 5.15* mostra a arquitetura inicialmente implementada nos *datacenters* da instituição Governamental, contendo numa primeira instância o servidor e os dois *proxys* para a monitorização dos equipamentos e serviços presentes nos *datacenters* da instituição. Foram, desde logo, estipulados os mecanismos de *backups* da própria infraestrutura de monitorização, garantindo assim uma maior resiliência em situações onde seja necessário recorrer aos *backups*. De igual modo, foi estipulado a política de retenção de backups do sistema de monitorização, onde foi definido o armazenamento total de todos os *backups* da última semana. O servidor central da plataforma *Zabbix* irá agregar toda a informação de monitorização da instituição Governamental, deste modo, foi estipulado fazer *backups* de três em três horas, minimizando assim o tempo de perda de informação em caso de reposição de um *backup*.

O processo de instalação da plataforma *Zabbix* nos *LXC Containers* foi efetuado com base na documentação oficial da própria plataforma. De maneira a garantir maior suporte a longo prazo, foi decidido a instalação do *Zabbix 6.0 LTS* (*Long Term Support*). Esta decisão garante o suporte da plataforma de monitorização até 28 de fevereiro de 2027. Para o motor de base de dados, foi utilizado o *software MariaDB*, onde de igual modo foi seguida a documentação oficial do mesmo no processo de criação da base de dados, utilizadores e respetivos privilégios. Os *proxys* foram configurados para funcionar no modo ativo, isto é, os *proxys* vão enviar as métricas recolhidas diretamente para o servidor *Zabbix*. Este mecanismo irá fazer com que se poupe recursos do lado do servidor, visto não ter de tratar do processo de '*polling*'. Nos anexos encontra-se informação detalhada e documentada do procedimento de instalação efetuado.

5.2.1. *Datacenters*

Os primeiros dispositivos a serem monitorizados foram todos os equipamentos pertencentes a ambos os *datacenters* da instituição Governamental. Para tal, foi efetuado o levantamento de todos os equipamentos presentes nestas infraestruturas, onde de seguida, definiu-se os grupos que irão ser criados na plataforma de monitorização. Estes grupos irão permitir uma segmentação de equipamentos/métricas de monitorização por *datacenters*, tipo de marca de dispositivo, tipo de serviços e *sites,* dando assim aos gestores de sistemas e redes uma forma estruturada e organizada para filtragem de informação de forma eficiente.

Foi delineada a utilização do agente *Zabbix LTS (Long Term Support)* para respetiva recolha e envio de informação na grande maioria da infraestrutura dos sistemas da instituição Governamental, nomeadamente servidores e sistemas de virtualização. Esta decisão teve por base os resultados obtidos na monitorização em servidores *Windows* e *Linux*, utilizando o agente *Zabbix* e outro utilizando o protocolo *SNMP (Simple Network Management Protocol)*. Verificou-se uma maior facilidade e escalabilidade nos dados obtidos a partir do agente *Zabbix* ao invés da utilização do protocolo *SNMP*. Face às suas autodescobertas *standard* presentes no agente *Zabbix*, este obteve informações quer a nível de *hardware* e *software* mais precisas nos servidores e sistemas de virtualização.

Face à situação exposta anteriormente, foi então embutido na arquitetura de monitorização a utilização, sempre que possível, do agente *Zabbix* para respetiva recolha e envio de informação entre o *proxy*, e os dispositivos tais como servidores e sistemas de virtualização.

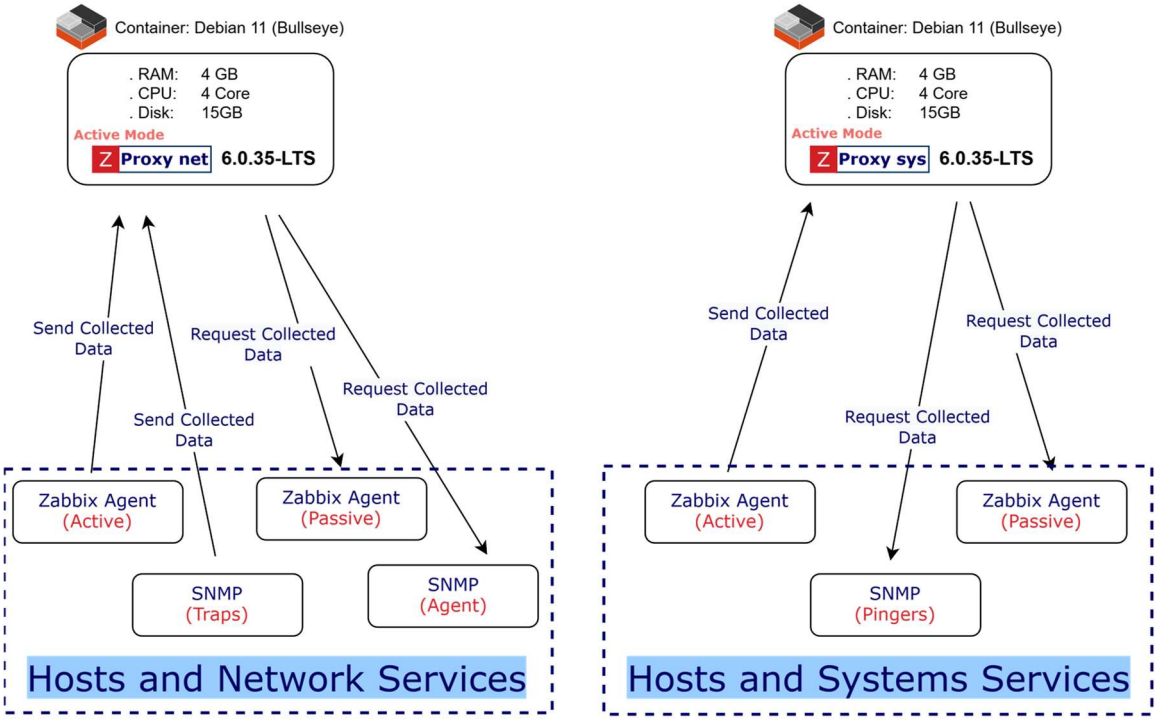

Figura 5.16: Arquitetura de recolha de métricas de monitorização nos *datacenters*.

A *Figura 5.16* mostra a definição base para a recolha das métricas de monitorização entre dispositivos e/ou serviços para com os proxys do *datacenter*. Ao nível dos equipamentos em que não é possível efetuar-se a instalação do agente *Zabbix*, como é o caso de *switches* e *routers*, foi estipulado a utilização do protocolo *SNMP (Simple Network Management Protocol)*. Face à criticidade e sensibilidade da informação dentro do *datacenter*, foi de igual modo estipulado a utilização do protocolo *SNMPv3,* garantindo deste modo a confidencialidade dos dados de monitorização.

Abaixo fica discriminado os parâmetros *standard* para a monitorização *SNMPv3*:

- SNMP version: **SNMPv3**
- Security Level: **authPriv**
- Authentication Protocol: **SHA256**
- Privacy Protocol: **AES128**

Para cada equipamento a ser monitorizado via *SNMPv3*, foi definida a não reutilização de *usernames* e *passwords* de autenticação, elevando desta forma os níveis de confidencialidade dos dados de monitorização.

5.2.2. *Sites* Rede Privativa

Após a monitorização da infraestrutura mais crítica da instituição Governamental, os *datacenters*, passou-se para a monitorização dos 265 *sites*. A máquina utilizada para *proxy*, foi um *Raspberry Pi3 model* B, com o sistema operativo *Debian 11 Bullseye*, que ficou instalado no *site*, para recolha de todas as métricas dos dispositivos e serviços de rede neste alojados.

Em reunião com os responsáveis pela gestão e monitorização da instituição Governamental, foi definido que métricas teriam de ser monitorizados, estando abaixo a discriminação destas, por categorias de equipamentos:

- ***Switches***:
  - *Uplinks*;
  - Largura de banda consumida;
  - Retransmissão de pacotes (*In* / *Out*);
  - *Uptime*;
  - Versão de *firmware;*
  - Anomalias de *hardware*;

- ***Routers***:
  - *Uplinks*;
  - Largura de banda consumida;
  - Retransmissão de pacotes (*In* / *Out*);
  - *Uptime*;
  - Versão de *firmware*;
  - Anomalias de *hardware*;

- **Impressoras**:
  - *Uptime*;
  - Níveis dos *tonners*;
  - Nível de Papel;
  - Versão de *firmware*
  - Anomalias de *hardware*;

- ***Access Points***:
  - *Uptime*;

A definição da monitorização das portas dos *switches,* apenas para os seus *uplinks*, advém da quantidade de notificações / alertas, que os gestores de sistemas e redes receberiam como, por exemplo, um utilizador a reiniciar o seu dispositivo.

Com base na definição dos parâmetros a monitorizar nos *sites* da instituição Governamental, foi configurado na plataforma *Zabbix* um grupo contendo todos os *sites* da instituição Governamental como podemos ver na *Figura 5.17*.

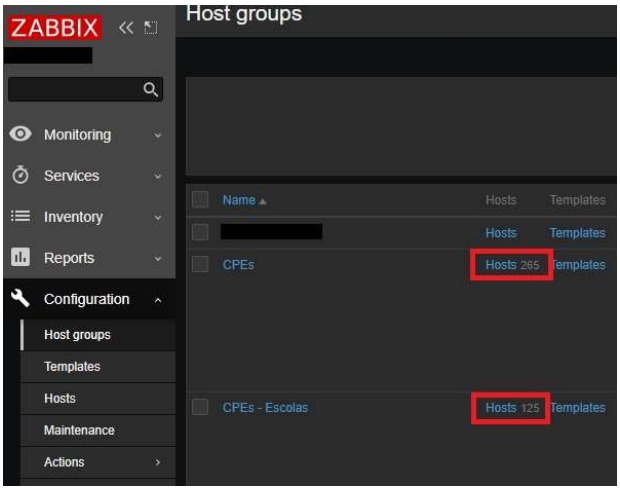

Figura 5.17: Criação dos grupos contento os *sites* da instituição Governamental.

Foi solicitado um novo requisito por parte dos responsáveis pela gestão e monitorização da instituição Governamental, nomeadamente a criação de um subgrupo, contendo todos os *sites* que contenham escolas básicas e secundárias da instituição. Assim, a organização dos grupos de *sites* da instituição ficou da seguinte forma

- **CPEs** – Grupo contendo todos os *sites* da instituição Governamental;
    - **CPEs – Escolas** – Subgrupo contendo todas as escolas básicas e secundárias da instituição Governamental;

Tal como referido anteriormente, cada *site* da instituição Governamental possui um *router* que interliga, por sua vez, à sua rede privativa. Para a monitorização dos *routers*, numa fase inicial, foi utilizado o *template* de base da plataforma *Zabbix,* através do protocolo *SNMP*. Após a conclusão da monitorização dos 265 *routers* dos *sites* da instituição Governamental, foram criados de raiz dois *templates*, para os dois modelos existentes de *routers*. Estes *templates* possuem de base os parâmetros inicialmente definidos pelos responsáveis pela gestão e monitorização da instituição, como podemos ver na *Figura 5.18*, como também reajustes na frequência com que determinadas métricas são obtidas, garantindo dados de monitorização mais precisos. Este aumento de frequência com que determinadas métricas são obtidas, permite notificar os gestores de redes de uma forma mais célere, quando é detetada alguma anomalia.

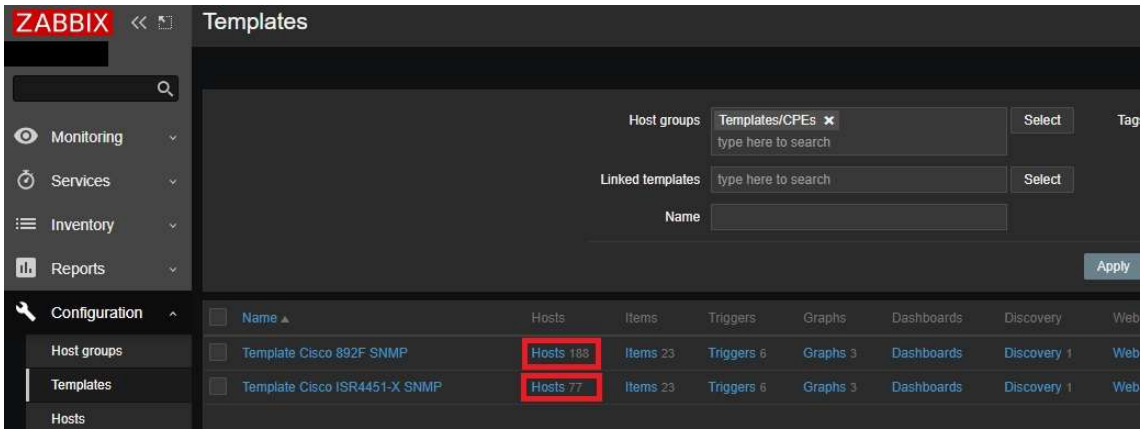

Figura 5.18: Templates criados para os tipos de *routers,* nos *sites* da instituição.

A *Figura 5.19* mostra as configurações efetuadas num dos *templates* dos *routers*, onde, tendo em conta o tipo de métrica e sua importância, a frequência com que esta é obtida foi incrementada. Inicialmente, estas métricas estariam a ser obtidas com uma frequência de 5 em 5 minutos, o que não permitiria aos gestores de redes, serem notificados de forma célere aquando de uma anomalia. Face às características do *Zabbix*, esta alteração foi aplicada em massa para todos os 265 *routers* da instituição, alteração essa, que teve um grande impacto na base de dados e no próprio servidor *Zabbix*. Com esta alteração, foi necessário aumentar a base de dados do servidor *Zabbix,* 8 vezes o inicialmente alocado, e efetuar ajustes avançados na própria base de dados como *cache* e número de *threads* alocados, face à demanda da quantidade de dados que estaria a processar. Na própria plataforma *Zabbix*, foi necessário efetuar-se *fine tuning* nas suas próprias configurações, alocando mais *threads* de acordo com o tipo de análise que é efetuado no servidor, isto é, no caso dos *routers* dos *sites* da instituição, como a sua monitorização tem por base o protocolo *SNMP*, foi necessário alocar mais *threads* ao servidor para a análise e processamento deste tipo de dados, diminuindo desta forma os tempos de *queue* no servidor, tal como representado na *Figura 5.20*.

As configurações de *fine tuning* na plataforma *Zabbix*, foram efetuadas tendo por base a análise de *logs* da própria plataforma. A documentação existente não sintetiza que valores deverão ser atribuídos consoante o tipo e quantidade de dados, tornando a sua configuração árdua.

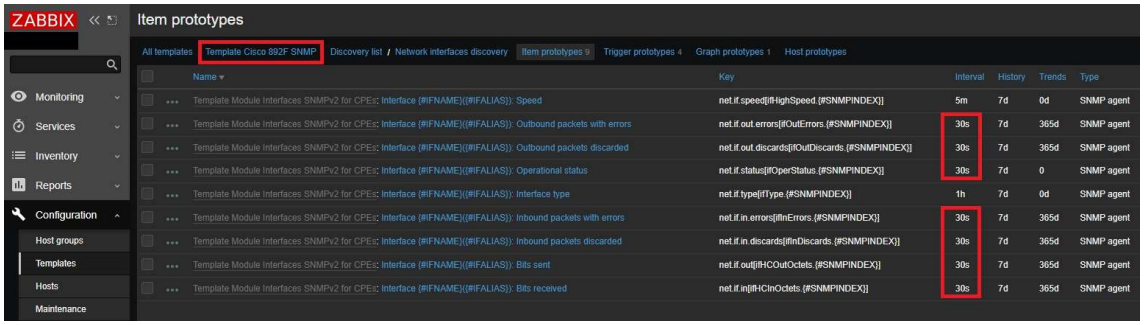

Figura 5.19: *Fine tuning* dos *templates* criados para os *routers* da instituição.

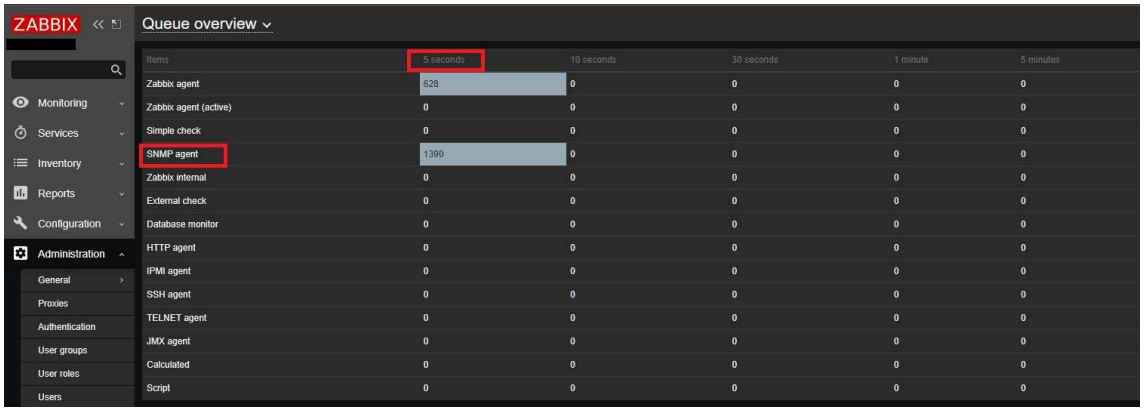

Figura 5.20: Visão geral da *queue* do servidor *Zabbix*.

Após a monitorização de todos os *routers* que constituem os 265 *sites* da instituição Governamental, foi criado um *dashboard* que agrega a informação de todos estes, demostrando de forma clara o seu estado geral. Este *dashboard* tem a particularidade de ser dinâmico, ou seja, informa problemas existentes nos *routers* da instituição é automaticamente lançada. Além desta particularidade, foi configurado um mapa com as ilhas atlânticas, onde através do *geomap*, possui-se a localização de cada *site* da instituição Governamental, com a representação dinâmica do seu correto funcionamento, auxiliando assim os gestores de redes a identificar que *sites* estão com problemas.

A forma como o *dashboard* foi organizado teve por base reuniões efetuadas com membros das equipas de redes da instituição Governamental, onde se definiu a representação visual apenas de situações críticas que colocassem em causa o seu funcionamento, como por exemplo a perda de comunicação de um *router*.

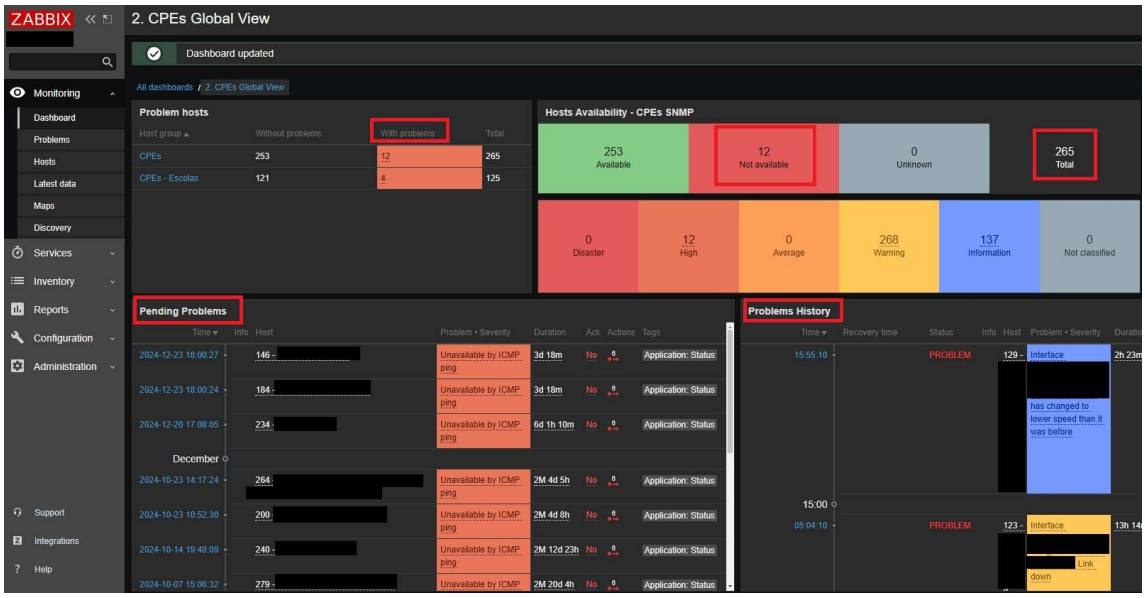

Figura 5.21: *Dashboard* dinâmico acerca dos 265 *routers* da instituição.

Com o avançar na monitorização, foi identificado desde logo um problema em todos os *sites* da instituição Governamental, pois não estava implementada a segregação das redes de gestão das de dados, fazendo com que a gestão dos equipamentos de rede estivesse junto com gestão das redes de dados. Esta situação causou grandes transtornos no processo de implementação, visto não ser viável a sua implementação face às características sobretudo complexidade e dimensão da rede privativa da instituição Governamental.

Deste modo, foi necessário elaborar um procedimento de padronização de todos os 265 *sites* da instituição Governamental, onde houve uma separação a nível de redes de gestão, como de redes padrões, como por exemplo, rede das impressoras, rede *access points*, rede *IoT* e *VoIP*.

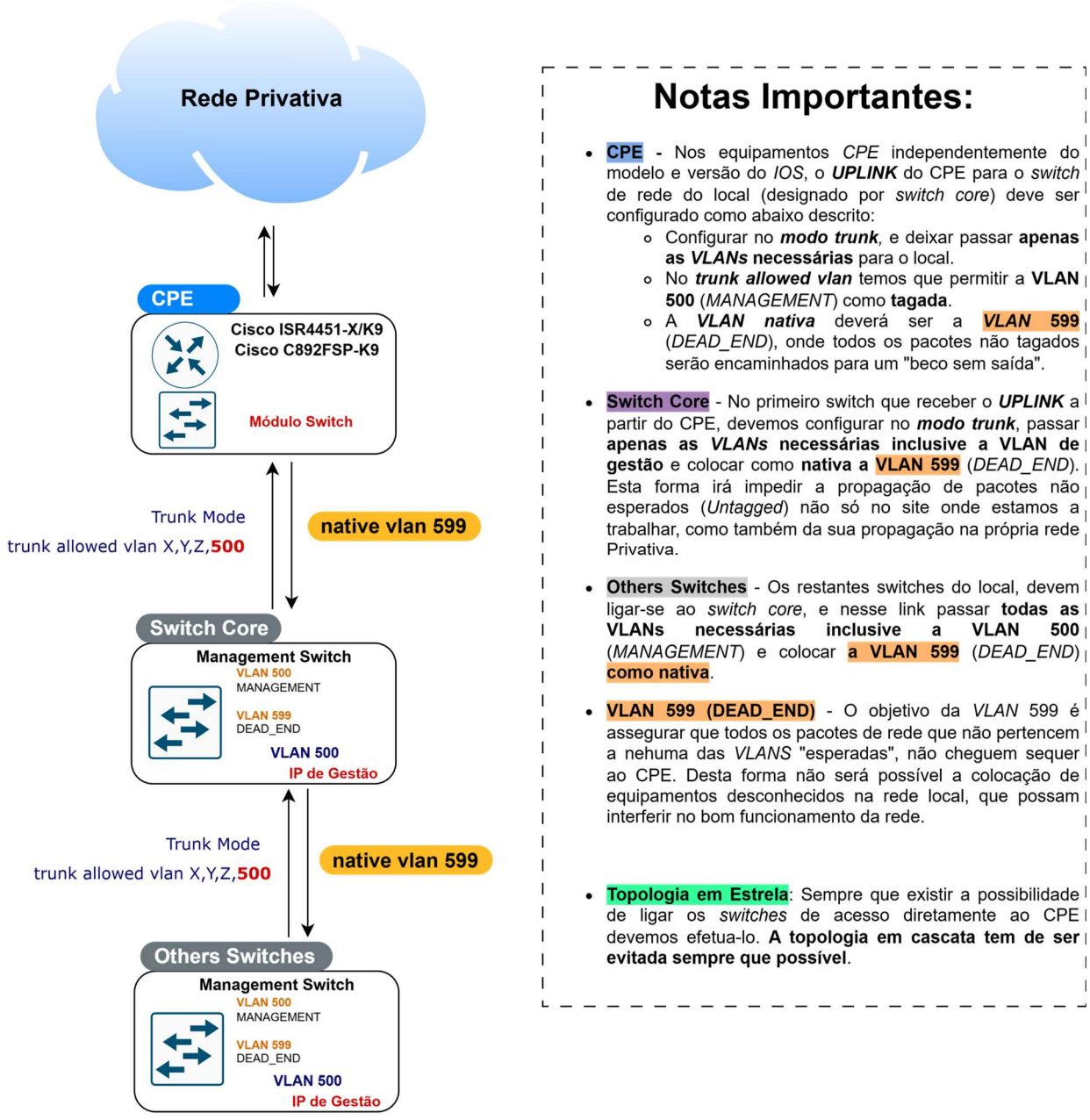

Figura 5.22: Procedimento para redes de gestão, dos *sites* da instituição.

A *Figura 5.22* mostra o procedimento elaborado para a segmentação e padronização dos 265 *sites* da instituição Governamental, a nível das redes de gestão dos equipamentos e/ou serviços. Foi também definido, aquando da correção da parte lógica dos equipamentos, a implementação sempre que possível da topologia de rede em estrela, como representado na *Figura 5.23*. Esta recomendação de topologia irá trazer uma maior resiliência e fiabilidade às redes internas de cada *site* da instituição Governamental, devido a não se possuir qualquer tipo de *switch* dependente de outro.

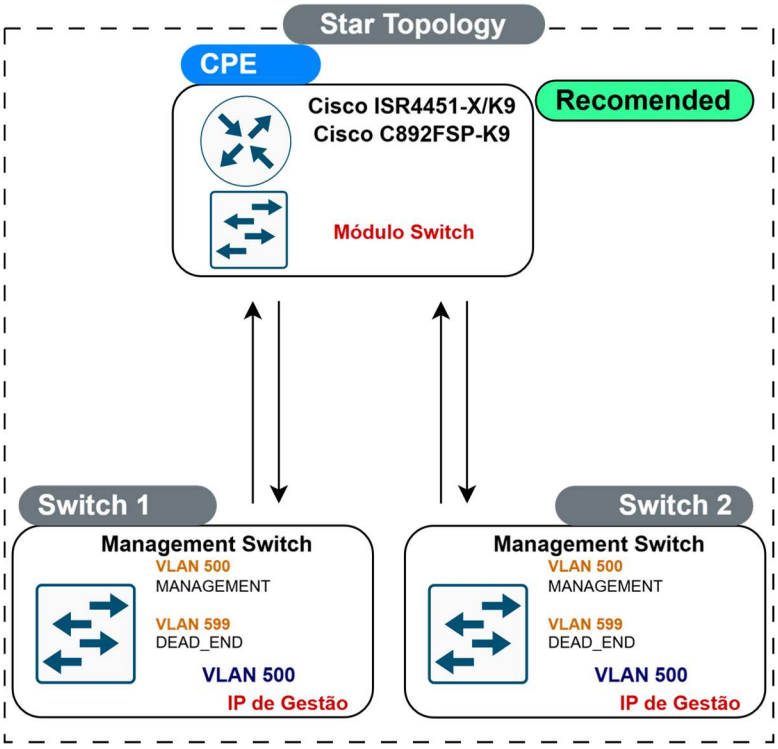

Figura 5.23: Recomendação da topologia dos *switches,* nos *sites* da instituição.

Outro ponto fundamental para a implementação da monitorização dos 265 *sites* de instituição Governamental, é a documentação das redes de gestão que são utilizadas ao longo dos seus *sites*. Este fator é importante, para uma correta gestão e monitorização de todos os equipamentos e serviços ao longo dos seus *sites*. Foi identificado que a instituição Governamental possuía lacunas na documentação das suas redes, tornando assim o processo de implementação da monitorização moroso.

Assim, foram implementados e definidos procedimentos de documentação das redes de toda a instituição Governamental, não só apenas dos *sites* remotos como também dos seus *datacenters*, com auxílio da plataforma *open-source Netbox*. Para a documentação total da infraestrutura de rede da instituição Governamental, foi necessário ir a cada um dos *sites* e documentar manualmente todos estes.

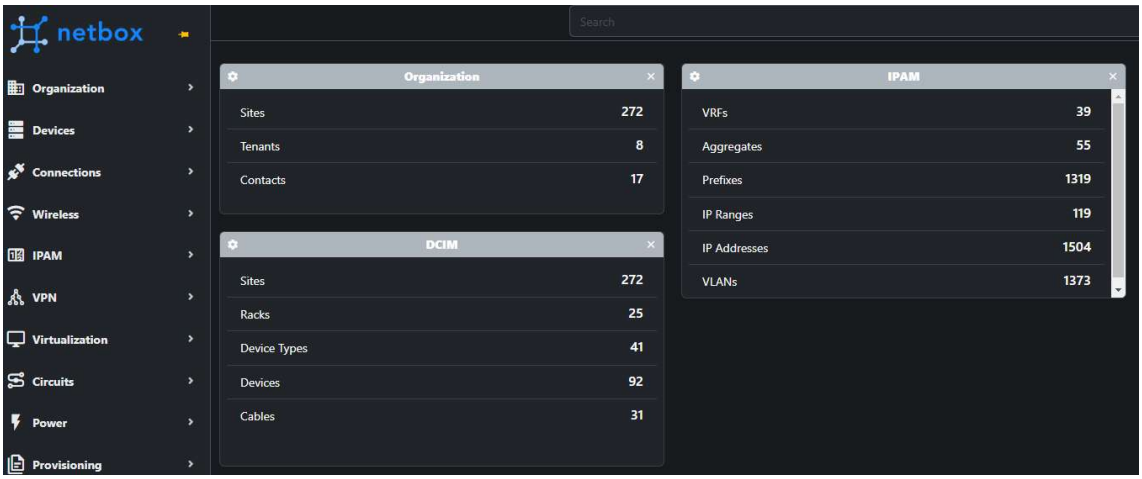

Figura 5.24: Visão geral da documentação na plataforma *Netbox*, da instituição.

Durante este processo de documentação, foram identificadas várias lacunas, como por exemplo a duplicação de endereçamentos de rede, redes *legacy* em produção entre outras mais. A *Figura 5.24* mostra a visão geral de todo o processo de documentação efetuado em toda a instituição Governamental onde, como podemos verificar, foram documentados mais de 1500 endereços *IP* ao longo de toda a sua infraestrutura, o que mostra bem a dimensão da rede.

Apesar da definição dos procedimentos, a sua correção nos 265 *sites* da instituição Governamental é um processo extremamente demoroso, face à sua pequena equipa e impacto que estas alterações trazem nos *sites*. Devido a esta situação, em reunião com os responsáveis pela gestão de monitorização da instituição Governamental, foi delineado numa fase inicial, efetuar-se a monitorização dos *sites* da instituição Governamental apenas dos seus *routers*, usando por base a arquitetura de monitorização centralizada.

5.2.3. Estrutura da Informação

A estrutura da informação dos dados de monitorização teve por lógica a segmentação dos *sites* remotos da sua rede privativa, os seus *datacenters* e todos os dispositivos e serviços em torno dos sistemas. A forma como os grupos foram delineados, foi para efetuar-se filtragens baseadas no tipo *AND*, de maneira que os gestores de sistemas e redes possam de forma rápida e clara, possuir toda a informação necessária, para um cenário em concreto. Deste modo, criou-se as seguintes categorias globais, na plataforma *Zabbix*, para a organização da informação de monitorização da instituição Governamental:

- **CPEs:**
  - **CPEs – Escolas;**

Este grupo e subgrupo, tal como explicado anteriormente, tem como objetivo identificar cada um dos 265 *sites* da instituição Governamental. Cada *site* possui um *ID* único interno da instituição, *ID* esse, que é utilizado para efetuar a designação do local**.**

- ***Datacenters:***
  - *Datacenter A;*
  - *Datacenter B;*

O grupo *datacenters* tem como finalidade, a fácil segmentação da informação de monitorização por *datacenter*. Esta abordagem tem como vantagem, a rápida listagem de todos os dispositivos e serviços dependentes de cada um dos *datacenters*.

- ***Network/Switches:***
  - *Switches – Aruba;*
  - *Switches – Cisco;*
  - *Switches – Ubiquiti;*
- **Network/Access Points:**
  - *Access Points – Ubiquiti;*
  - *Access Points – Aruba;*
  - *Access Points – TP-Link;*
- ***Network/Routers:***
  - *Routers – Cisco;*

Os dispositivos de rede estão estruturados baseados no tipo de equipamento e respetiva marca. Esta forma de organização, tem como objetivo a rápida listagem de equipamentos de uma dada marca ao longo de toda a instituição Governamental.

- **Servidores:**
  - Servidores – *Windows;*
  - Servidor – *Linux;*
- ***Storage****:*

- ***Containers***:
  - *LXC Containers;*
  - *Docker Containers;*
- **Máquinas Virtuais:**
  - Máquinas Virtuais – *Windows*;
  - Máquinas Virtuais – *Linux;*
- **Servidores *Web:***
  - *Web Engine – Apache;*
  - *Web Engine – Nginix;*
  - *Web Engine – Tomcat;*
  - *Web Engine – IIS;*

Por fim, os grupos associados aos sistemas foi estruturado com base no tipo de dispositivos e serviços. Este possui mais categorias comparativamente aos anteriores, visto que, no caso dos sistemas, a estrutura da informação foi desde a camada de servidores à camada aplicacional.

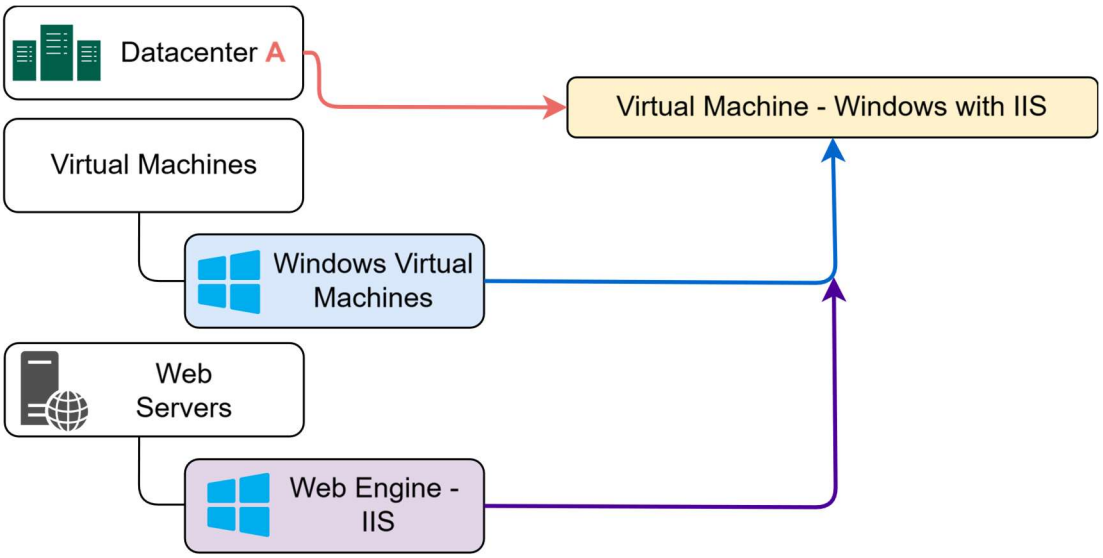

Figura 5.25: Exemplo prático da finalidade da estrutura da informação.

A *Figura 5.25* mostra um exemplo prático de como a estrutura da informação efetuada funciona, no caso dos sistemas, onde tem-se uma máquina virtual com serviços *web* instalados. Podemos verificar que, com esta forma da organização, é possível os administradores de sistemas e redes efetuam filtragens por dados de monitorização por dispositivos ou por serviços, de forma fácil e intuitiva. Permite também responder a uma nova demanda na instituição Governamental, que é ter o inventário de todos os *softwares* instalados em seus *datacenters,* para uma maior celeridade em resolver problemas de segurança relacionados com *CVE* (*Common Vulnerabilities and Exposures*).

5.2.4. *Templates*

Desde cedo, em reuniões com os responsáveis pela gestão e monitorização da instituição Governamental, foram estipulados *templates* de monitorização muito específicos tendo em conta a natureza própria que alguns sistemas possuem para a disponibilização de serviços a seus clientes. Deste modo, desde o início da implementação da plataforma *Zabbix*, foram desenvolvidos *templates* de monitorização específicos para *windows server*, *hipervisors*, *domain controllers* e *print servers*. Além da monitorização essencialmente baseada no sistema operativo, foi também definida a monitorização de serviços considerados relevantes para o dia-a-dia da instituição Governamental, como é o caso dos motores *web*, bases de dados e serviços muito específicos como, por exemplo, *tomcat.*

Na plataforma *Zabbix* os *templates* criados foram organizados em grupos, baseados no tipo de serviço a que pertenciam. Abaixo fica a lista de alguns *templates* e grupos criados e configurados na plataforma *Zabbix*:

- ***Templates/Operating System:***
  - *OS Hyper-V Server by Zabbix Agent;*
  - *OS Proxmox by Zabbix Agent;*
  - *OS Linux by Zabbix Agent;*
  - *OS Linux by Zabbix Agent Active;*
  - *OS VM Windows server by Zabbix Agent;*
  - *OS VM Windows server by Zabbix Agent Active;*
- ***Templates/Applications:***
  - *Windows IIS server by Zabbix Agent;*
  - *Apache server by Zabbix Agent*
  - *Nginx server by Zabbix Agent;*
  - *Windows Print server by Zabbix Agent;*
  - *Windows Domain Controller by Zabbix Agent;*
- ***Templates/LXC Containers:***
  - *LXC Container by Zabbix Agent;*
  - *LXC Container by Zabbix Agent Active;*
- ***Templates/Storage:***
  - *QNAP by SNMP;*
  - *NetApp AFF by SNMP;*
  - *NetApp FAS by SNMP;*
- ***Template/Power Systems:***
  - *APC Smart-UPS by SNMP;*
  - *APC PDU by SNMP;*
- ***Template/Printers:***
  - *Cannon C5540 by SNMP;*
- ***Template/Routers:***
  - *Cisco 892F by SNMP;*
  - *Cisco ISR4451-X by SNMP;*
- ***Template/Network Devices:***
  - *Cisco Switches by SNMP;*
  - *TP-Link Switches by SNMP;*
  - *Unifi Switches by SNMP;*
  - *Unifi Access Point by SNMP;*
  - *Aruba Acces Point by SNMP;*

A grande maioria dos *templates* usou de base os disponibilizados pela plataforma *Zabbix* e outros a partir da própria comunidade *Zabbix*. Os *templates* foram alterados de acordo com as necessidades inicialmente definidas pelos responsáveis pela gestão e monitorização da instituição, como também pelas equipas de redes e sistemas da instituição, como por exemplo o tempo para ser enviado um alerta, em caso de situação crítica.

A *Figura 5.26* representa, de forma resumida, como foi definida a associação de *templates* aos servidores, a qual teve por base o tipo de servidor e sistema operativo. Os *templates* baseados em sistema operativos foram profundamente modificados face à quantidade de dados de monitorização que não acrescentavam valor. A título de exemplo o serviço *windows update*, despoletava alertas quando este serviço terminava a sua função, não trazendo qualquer tipo de valor à monitorização.

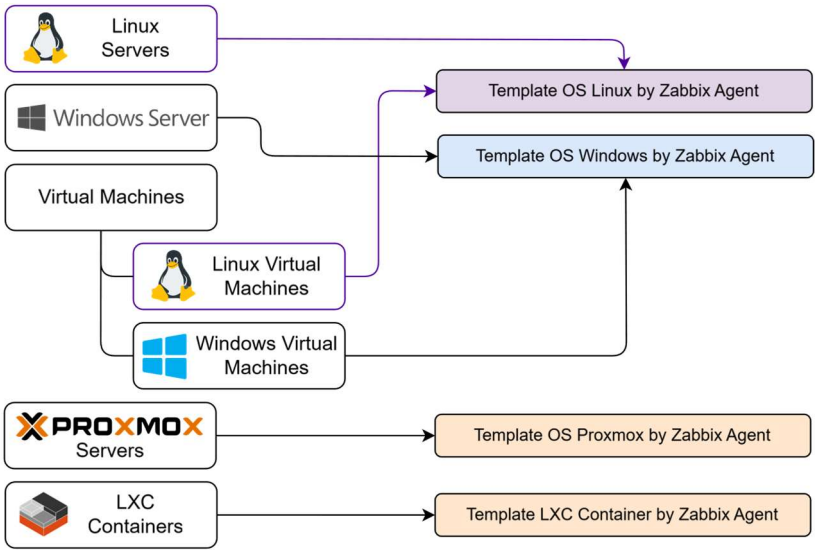

Figura 5.26: Associação de *templates* consoante o tipo de servidor.

Ao longo da implementação, foi necessário efetuar ajustes nos *templates* utilizados, de maneira a garantir uma maior eficiência de armazenamento. Tem-se, como exemplo, apenas registar o dia e hora que o dispositivo se desligou e não guardar na base de dados continuamente que este está "*online*". Estes pormenores foram tidos em consideração e tiveram grande impacto na dimensão da base de dados. A *Figura 5.27* mostra como exemplo uma destas configurações onde, para o caso do *template* dos *LXC Containers*, existe uma métrica de monitorização que regista a última data que o *Container* reiniciou, onde só armazena efetivamente as datas de *boot* aquando existe um reiniciar.

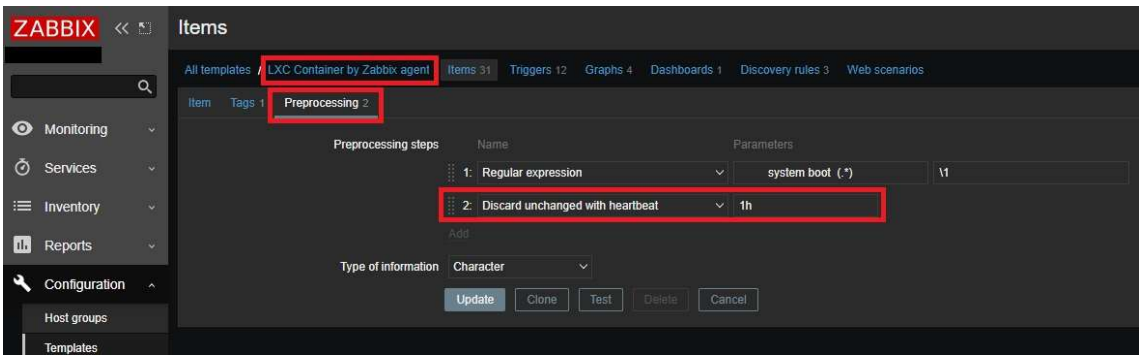

Figura 5.27: Exemplo otimização da base de dados no *template*.

Nos *templates* criados foi necessário efetuar-se ajustes nos *triggers*, face à criticidade de alguns destes para o bom funcionamento da instituição Governamental. A *Figura 5.28* mostra como exemplo, a configuração de um *trigger* para servidores *windows*, que possuem o sistema de virtualização *Hyper-V* e faça parte do *cluster* da instituição. Com base em reuniões com a equipa de sistemas, existiu a necessidade de efetuar a monitorização de um parâmetro do *cluster*, parâmetro esse que informa sobre o atual funcionamento do servidor no *cluster*. A consequência deste serviço com anomalia, poderia significar todo o *cluster* da instituição parar, face à sua criticidade o alerta foi categorizado como *high*.

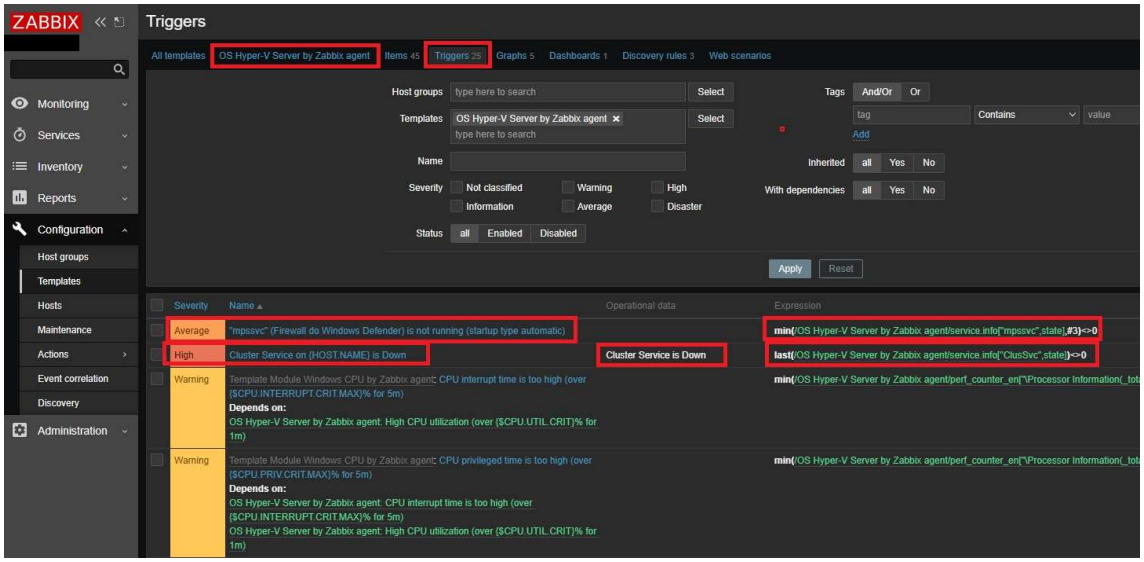

Figura 5.28: Criação de *triggers* específicos consoante a criticidade.

Os *templates* criados seguiram as *guidelines* da documentação da plataforma *Zabbix*, efetuando associações entre estes. Estas associações irão permitir, de uma forma centralizada, efetuar alterações em massa. A *Figura 5.29* representa o diagrama geral de um dos *templates* criados de raiz para a instituição com respetivas associações.

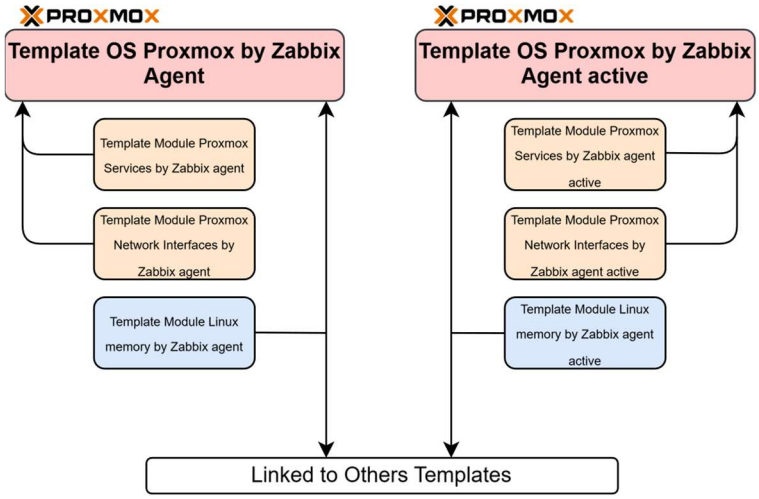

Figura 5.29: Exemplo de *template* criado com associação a outros *templates*.

5.2.5. Notificações e Alertas

A instituição governamental utiliza como meio de comunicação principal os serviços da *Microsoft*, onde a alarmística foi integrada com os seus serviços. A equipa técnica que possui a responsabilidade da manutenção e monitorização da infraestrutura da instituição Governamental, definiu que um dos métodos a receber a alarmística por parte da monitorização, será através de um canal no *Microsoft Teams*, onde foi definido sete categorias para os tipos de notificações / alertas nomeadamente:

- ***CPEs:***
  - *Routers* de cada um dos *sites* da instituição Governamental;
- ***Firewalls:***
  - Dispositivos que constituem a arquitetura das *firewalls*;
- ***Power Systems;***
  - Equipamentos elétricos presentes nos *datacenters*;
- ***Servers:***
  - Servidores físicos e virtuais presentes nos *datacenters*;
- ***Storages:***
  - Equipamentos de armazenamento presentes nos *datacenters*;
- ***Switches:***
  - Equipamentos de *switching* presentes nos *datacenters*;
- ***Websites:***
  - Monitorização dos *sites* da instituição Governamental;

Deu-se principal foco à monitorização dos *datacenters* da instituição, face ao facto de estes serem o ponto central para a disponibilização de todos os serviços, para os seus 265 *sites* espalhados ao longo da sua rede privativa. Foi, de igual modo, definido apenas receber notificações / alertas com a categoria de *disaster*, *high* e *average* no canal do *Microsoft teams* e, para notificações críticas, foi configurado outro meio de notificação, através do *telegram* com a utilização de *bots*, para que os gestores de sistemas e redes sejam notificados a partir do seu telemóvel.

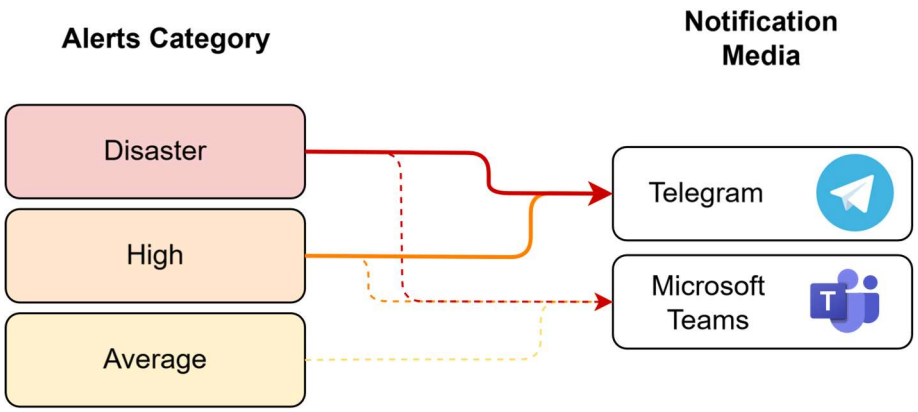

Figura 5.30: Definição do meio de notificação, com base no tipo de alerta.

A *Figura 5.31* mostra a configuração efetuada integrando a plataforma *Zabbix* com a plataforma de comunicação *Microsoft Teams*. Esta integração tem como finalidade atribuir acesso a utilizadores que, de acordo com as suas responsabilidades na instituição, terão meios de serem notificados aquando de uma anomalia onde é necessário a sua intervenção, diminuindo o tempo com que determinados serviços ficam indisponíveis aos seus utilizadores.

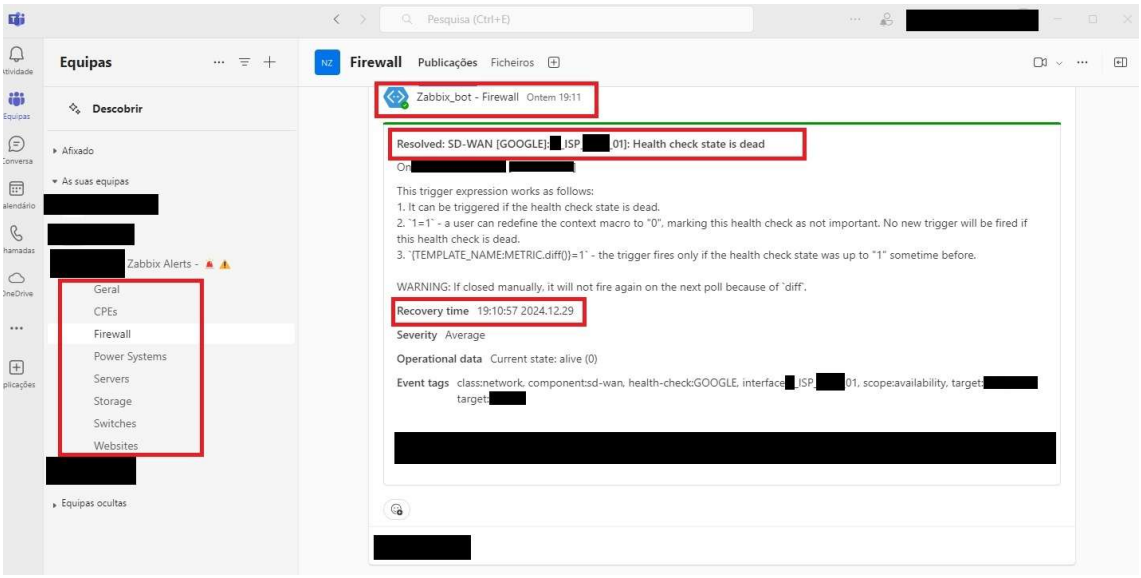

Figura 5.31: Notificações da monitorização, com integração no *Microsoft teams*.

Na *Figura 5.32,* mostra a integração efetuada na plataforma de comunicação *Telegram*, onde foi configurado pormenores como ícones a verde e a vermelho, para auxiliar os gestores de sistemas e redes a relatar efetivamente que dispositivos e/ou serviços estão com anomalias e se estes já foram ultrapassados.

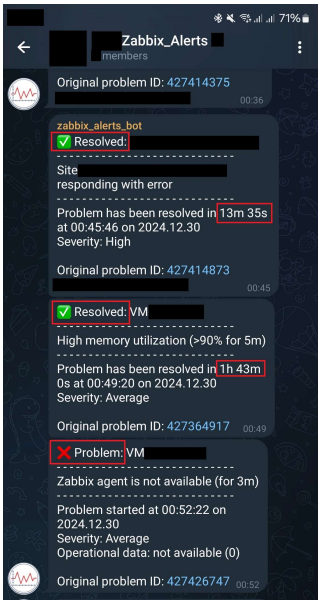

Figura 5.32: Integração efetuada com a plataforma de comunicação *Telegram*.

5.3. Visualização Gráfica

A informação de toda a monitorização da instituição Governamental, foi tratada e exposta ao longo de vários *dashboards* dinâmicos, com finalidades específicas de acordo com as necessidades dos administradores de sistemas e redes. Estes *dashboards* ao longo do tempo sofreram alterações, tendo por base reuniões com os gestores de cada área, tornando-os mais minimalistas, contudo mostrando dados agregados que dessem a visibilidade de toda a infraestrutura da instituição Governamental.

Assim foram criados vários *dashboards* que demostram dados agregados de toda a infraestrutura da instituição, onde vamos abordar os considerados mais críticos:

- *Internet* de toda a instituição Governamental;
- Arquitetura de *firewalls* de ambos *datacenters*;
- Serviços críticos para os 265 *sites* da instituição Governamental;
- Infraestrutura core dos *datacenters*;

Na *Figura 5.33* tem-se a representação global dos vários *links* de acesso à *internet* da instituição Governamental, de ambos os seus *datacenters*. A construção deste *dashboard* foi, no seu topo, apresentar o histórico de problemas agregados, onde caso o gestor de sistemas e redes pretenda efetuar uma correlação de eventos, o *dashboard* já está preparado para auxiliar nesse sentido. Os *dashboards* são dinâmicos, fazendo com que, em caso de anomalia num dos *links* de acesso à *internet*, este automaticamente irá mudar os estados de *alive,* representado a verde, para *down* ficando este representado a vermelho. Esta forma simples de representar os dados de monitorização, permite aos gestores de sistemas e redes, facilmente identificar as anomalias e suas consequências para a instituição Governamental.

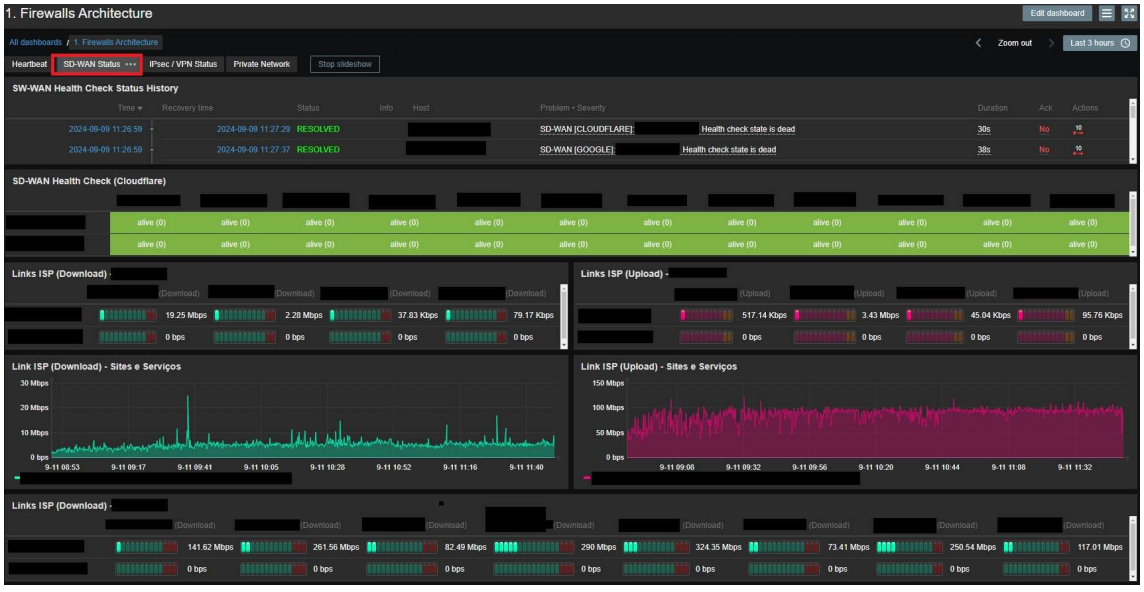

Figura 5.33: *Dashboard* com estado global dos acessos à *internet* da instituição.

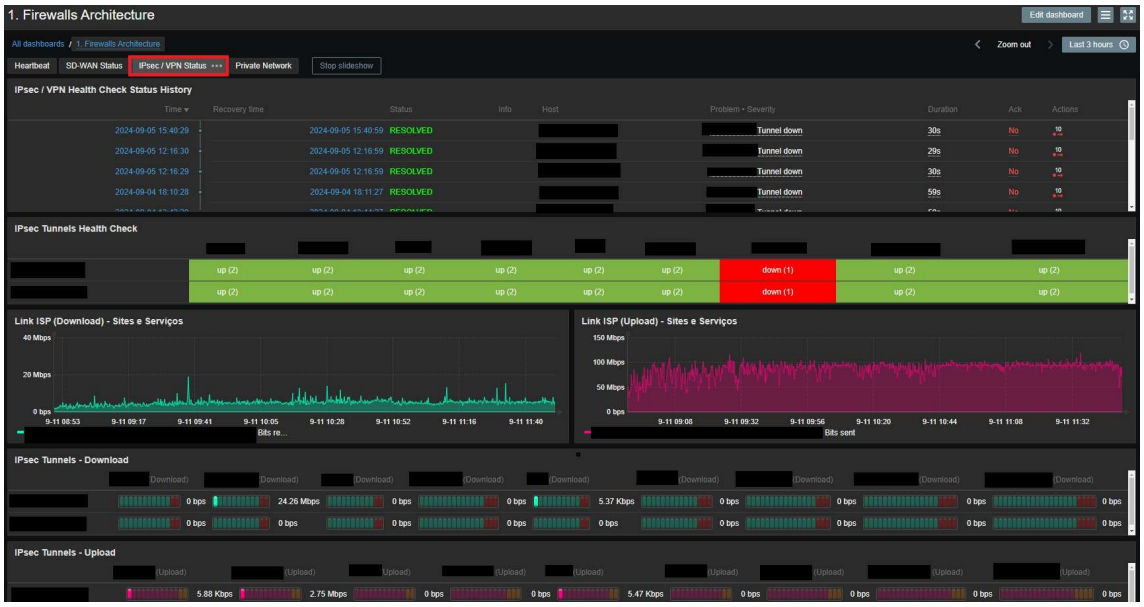

Figura 5.34: *Dashboard* com estado global dos tuneis *IPsec* da instituição.

Outro *dashboard* criado, *Figura 5.34*, e considerado crítico para o funcionamento normal da instituição, são as várias ligações a outras instituições / serviços através de túneis *IPsec*. A criação deste *dashboard* seguiu as mesmas características que as dos *links* de acesso à internet, onde neste podemos constatar a representação visual de um dos túneis *IPsec* em baixo, representado a vermelho com o termo *down*.

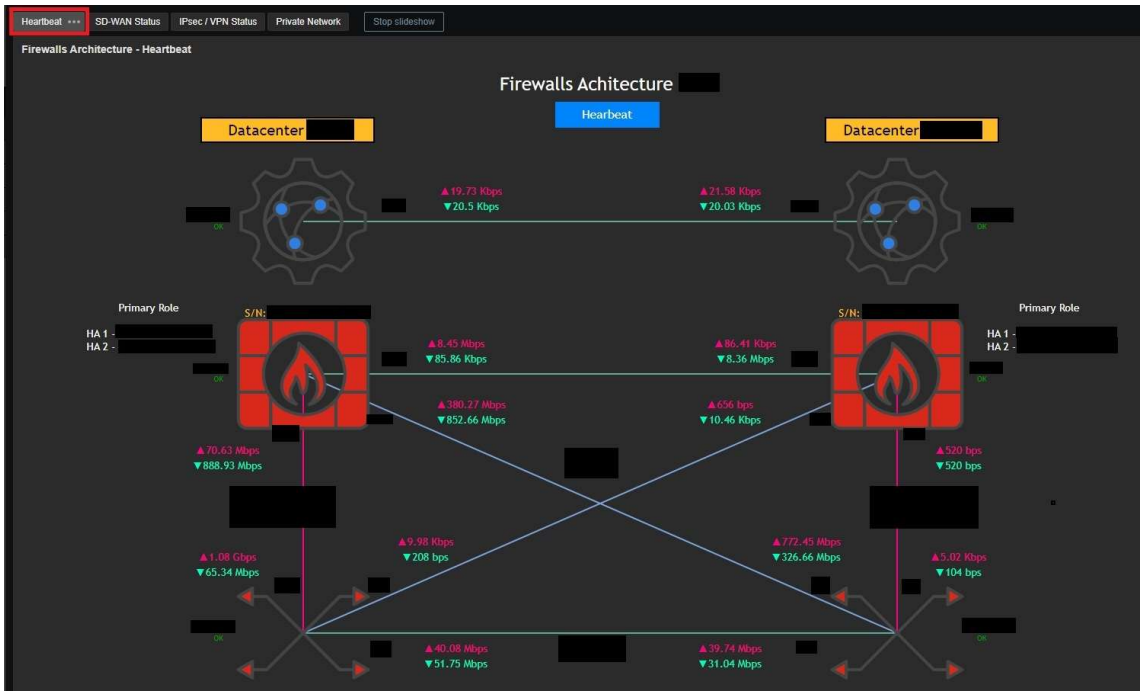

Figura 5.35: *Dashboard* com visão global da arquitetura de *firewalls* da instituição.

A *Figura 5.35* demostra toda a infraestrutura de *firewalls* da instituição, de ambos *datacenters*, onde foram representados todos seus *links* de ligação. Estes reagem dinamicamente em caso de anomalia, informando os gestores de redes mais precisamente para a causa da situação.

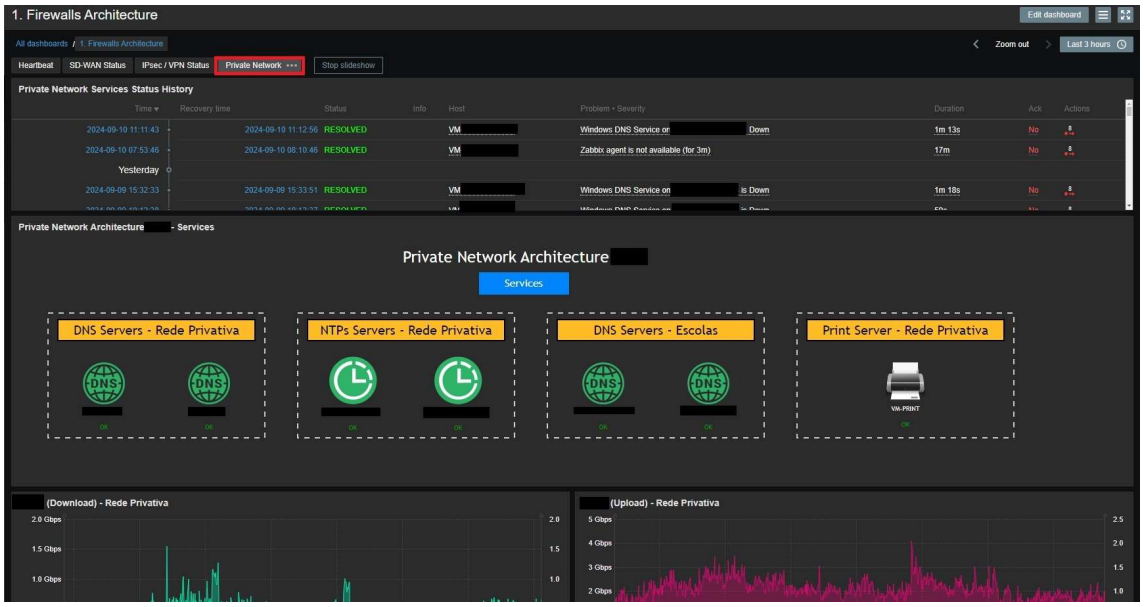

Figura 5.36: *Dashboard* com serviços críticos para os 265 *sites* da instituição.

A *Figura 5.36* representa o *dashboard* criado com os serviços categorizados como críticos para o normal funcionamento dos 265 *sites* da instituição Governamental. Os serviços considerados críticos são serviços que têm impacto direto nos mais de 5 mil utilizadores da rede privativa, como por exemplo *DNS* (*Domain Name System*) em secretarias e escolas, servidores de relógio e o servidor central de impressões da instituição. Tal como os *dashboard* anteriores, este é dinâmico alterando a sua representação visual de cada um destes serviços, quando é detetado uma anomalia.

A monitorização de serviços críticos dos *datacenters* da instituição, como as *UPS (Uninterruptable Power Supply)* e temperaturas, foram tidas em conta na elaboração de um *dashboard* específico, que representa o estado geral de ambos os *datacenters*. A *Figura 5.37* representa as temperaturas de ambos os *datacenters*, onde foi tido em consideração a representação das zonas quentes e zonas frias destes.

Figura 5.37: *Dashboard* com as temperaturas de ambos *datacenters* da instituição.

5.4. Conclusão

Este capítulo discriminou e contextualizou a pesquisa efetuada de plataformas de monitorização, como plataformas propícias à solução de arquitetura de monitorização para a instituição Governamental. Após o estudo e análise comparativa das várias plataformas propostas, foi delineada a decisão entre as duas plataformas *Nagios Core* e *Zabbix*. Para o apuramento final, foi estipulado junto com os responsáveis pela gestão e monitorização da instituição Governamental, os requisitos considerados prioritários, para poder-se efetuar-se a comparação entre ambas as plataformas. Após análise final, verificou-se que a plataforma *Zabbix* foi selecionada a implementar como solução, a arquitetura de monitorização da instituição Governamental. Foi sintetizado o funcionamento da arquitetura da plataforma de monitorização *Zabbix*, quais os seus componentes principais e como estes interagem entre si, demostrando funcionalidades e capacidades da plataforma, pertinentes para a implementação na instituição.

A configuração da plataforma *Zabbix* na infraestrutura da instituição Governamental, iniciou-se na parte *core* da proposta da arquitetura, a qual teve por base o servidor e os dois *proxys*, para ambos os *datacenters*. Foram estabelecidos os meios de comunicação, entre servidor e proxys, como também políticas de *backups* da infraestrutura de monitorização. Após a configuração da base de monitorização da plataforma *Zabbix*, efetuou-se a monitorização de ambos os *datacenters* da instituição, onde se definiu a utilização sempre que possível do agente *Zabbix* e a utilização do protocolo *SNMP*, com medidas que salvaguardem a confidencialidade dos dados.

A monitorização dos *sites* da rede privativa da instituição Governamental demostrou fragilidades nas suas redes de gestão, onde não existia qualquer tipo de segregação destas, com as redes de dados existentes. Esta situação fez com que fosse necessário efetuar-se a definição de procedimentos de padronização e documentação, para todos os 265 *sites* da instituição Governamental, desde a segmentação lógica de redes, como de topologias de rede recomendadas. Esta situação trouxe grandes transtornos à implementação da monitorização distribuída dos *proxys*, ao longo dos 265 *sites* da instituição, levando a uma tomada de decisão junto com os responsáveis pela gestão e monitorização da instituição Governamental, a efetuar-se numa primeira instância a sua monitorização tendo por base a arquitetura centralizada.

A estrutura de informação de toda a monitorização da instituição teve por base a definição de grupos e subgrupos, baseados em dispositivos e/ou serviços. Abordou-se a definição e utilização dos *templates*, como estes foram alterados baseados no tipo de criticidade, como também os sistemas de notificação e alerta. Por fim, demostrou-se a criação dos *dashboard* dinâmicos, que tiveram por base os serviços críticos da instituição Governamental.

De seguida, o próximo capítulo apresentará a análise e resultados, da implementação da arquitetura de monitorização distribuída na instituição Governamental, tendo por base as métricas recolhidas ao longo dos vários meses.

6. Análise e Resultados

Este capítulo pretende efetuar uma análise da arquitetura implementada na infraestrutura da instituição Governamental, validar com base nos resultados obtidos se a solução suprimiu os problemas / necessidades da instituição a nível de monitorização, apresentando critérios de avaliação de suporte.

Atualmente a, monitorização está a recolher e a analisar cerca de 80 mil métricas por segundo, onde engloba toda a infraestrutura da instituição Governamental, incluindo os dois *datacenters* e os *routers* dos seus 265 *sites*.

As próximas secções irão sintetizar a análise da proposta arquitetural de monitorização para a instituição Governamental (6.1), a reflexão sobre a monitorização dos *datacenters* (6.2), os seus *sites* da rede privativa (6.3), como a estrutura da informação auxiliou os gestores da instituição (6.4), como estes estão a receber, com base na plataforma de monitorização as notificações / alertas (6.5) e, por fim, o tratamento dos dados de monitorização e como estes são expostos, para auxiliar a análise das equipas de gestão da instituição Governamental (6.6).

6.1. Arquitetura

A arquitetura atualmente implementada na instituição Governamental possui um misto, onde no caso dos *datacenters* possui uma monitorização distribuída e, no caso dos *sites* remotos da instituição, possui monitorização centralizada.

Para análise da proposta arquitetural, foram implementados em dois *sites* da rede privativa da instituição Governamental, dois proxys para respetiva monitorização. O intuito destes *proxys* é efetuar-se uma comparação com as métricas de monitorização a partir dos *datacenters,* com as métricas a partir do *site*. O esperado teórico é obter umas métricas muito similares, face ao facto de a instituição Governamental possuir uma rede privativa interna. Deste modo, definiu-se os seguintes parâmetros para comparação das métricas obtidas:

- Tempo de latência;
- Tráfego de monitorização;
- Resiliência perdas de comunicação;

Existe a nuance em caso de falha da rede privativa, onde a monitorização dos *sites* a partir dos *datacenters* fica comprometida, ao invés de uma monitorização com a utilização de um *proxy* no *site*. Em caso de falha da rede privativa, o *proxy* continua a recolher métricas de monitorização e guarda estas localmente e, após retornar comunicação com o servidor central, envia-as estas para que possam ser processadas. Esta característica é considerada a maior diferenciadora, no caso particular da instituição Governamental, da abordagem de monitorização centralizada da de distribuída.

Site 1 – Aproximadamente 200 trabalhadores.

	Latência	**Tráfego de Monitorização**	**Resiliência**
Proxy	0.1*ms*	184*Kbps*	Independente da rede privativa
Centralizada (*datacenter*)	0.39*ms*	240*Kbps*	Dependente da rede privativa

Tabela 3: Comparação de monitorização *site* 1, centralizada e distribuída.

Site 2 – Aproximadamente 50 trabalhadores.

	Latência	**Tráfego de Monitorização**	**Resiliência**
Proxy	0.1*ms*	47*Kbps*	Independente da rede privativa
Centralizada (*datacenter*)	0.31*ms*	80*Kbps*	Dependente da rede privativa

Tabela 4: Comparação de monitorização *site* 2, centralizada e distribuída.

As *Tabelas 3 e 4*, mostram a comparação efetuada na monitorização dos *routers* de cada *site*, usando a abordagem centralizada e distribuída com uso de um *proxy*. Efetuando uma análise das tabelas, conclui-se que o ponto diferenciador das duas abordagens, relativamente à rede da instituição Governamental, está definido sobre dois parâmetros nomeadamente, tráfego de monitorização a ser enviado pela rede privativa e dependência da monitorização dos *sites* da própria rede privativa. Os valores de latência obtidos dão informação apenas do tempo de resposta desde o *datacenter* ao referido *site*.

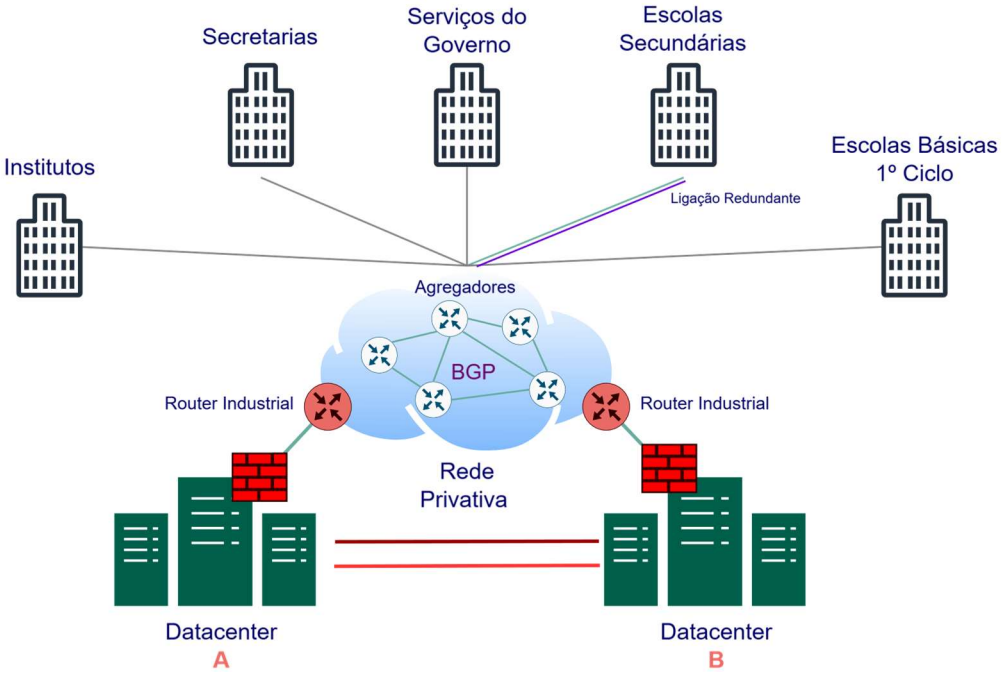

Figura 6.1: Interligação rede privativa aos *datacenters*.

A *Figura 6.1*, mostra a arquitetura global de funcionamento da rede privativa da instituição Governamental, onde como explicado anteriormente, todo o tráfego dos 265 *sites* da instituição, é dirigido sempre para os *datacenters*. A rede privativa tem por base uma arquitetura centralizada, isto é, todo o tráfego inclusive interno de cada *site*, é direcionado sempre para os *routers / firewalls* presentes nos *datacenters* da instituição. Esta é a forma como a instituição possui mecanismos de inspeção de segurança para todos os seus 265 *sites*, contudo esta arquitetura faz com que a proposta de arquitetura de monitorização distribuída possua apenas relevo no melhoramento da quantidade de tráfego de monitorização que é enviado ao longo da rede privativa até aos seus *datacenters*, e o acrescento de uma resiliência face a não estar dependente da infraestrutura da rede privativa da instituição Governamental, isto é, permite a alocação temporária dos dados de monitorização nos *proxys,* mesmo em caso de perda de comunicação com os *datacenters* da instituição.

6.2. *Datacenters*

Com a monitorização dos *datacenters* da instituição Governamental, permitiu possuir-se uma maior noção dos recursos disponíveis e indicadores de qualidade da sua infraestrutura. Os *proxys* dedicados para a monitorização dos sistemas e redes, permitiu efetuar ajustes a nível da plataforma *Zabbix*, consoante o tipo de métricas de monitorização, mas também auxiliar no processo de definição de procedimentos, tanto para as equipas de sistemas como para as equipas de redes.

A monitorização de ambos *datacenters* da instituição Governamental, encontra-se em produção desde novembro de 2021, incluindo todos os seus servidores físicos, virtuais e equipamentos de rede. Foi implementada a monitorização de equipamentos considerados críticos, pertencentes aos *datacenters*, como é o caso das *UPS (Uninterrupltible Power Supply)* e sistemas de ar condicionado. A monitorização destes sistemas críticos permitiu aos gestores de sistemas e redes saber o estado destes equipamentos, como também prever, em situações anómalas ao funcionamento do *datacenter*, quanto tempo de intervenção possuem até existência de quebra de serviços. A monitorização deste tipo de equipamentos permitiu, de igual modo, implementar medidas corretivas para um balanceamento de carga térmica e elétrica nos *datacenters* da instituição, melhorando a eficiência e fiabilidade dos próprios *datacenters*. A *Figura 6.2*, mostra o tempo que uma das *UPS* presentes num dos *datacenters* da instituição possui em caso de falha elétrica, dando informações úteis aos gestores de sistemas e redes.

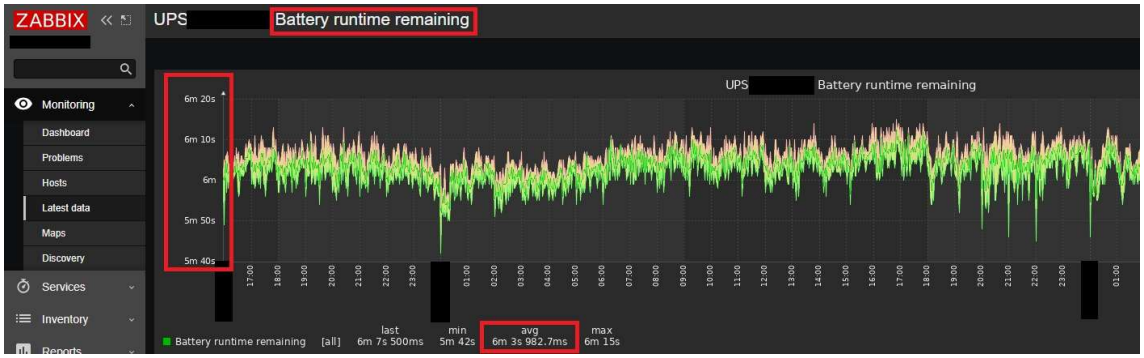

Figura 6.2: Gráfico de monitorização das *UPS* nos *datacenters*.

A monitorização dos *datacenters* da instituição Governamental, permitiu evidenciar várias lacunas existentes, que levavam à perda de *performance* e/ou à quebra de serviços. Estas situações surgiram tendo por base a monitorização implementada e a respetiva correlação dos dados de monitorização, com as configurações dos equipamentos e/ou serviços. Estas irregularidades fizeram com que fosse necessário elaborar novas arquiteturas de implementação nos *datacenters* da instituição Governamental, arquiteturas essas corretivas, desde a camada física à aplicacional.

Uma das situações anómalas detetadas foi nos *switches core* dos *datacenters* da instituição Governamental, os quais não tinham configurações a nível de *STP* (*Spanning Tree Protocol*), fazendo com que, por cada *1Gbs* de tráfego efetuado nos *datacenters*, 800*Mbs* seria descartado devido ao *STP*. Esta situação causava grandes transtornos a nível de *performance*, principalmente quando os seus servidores de armazenamento efetuavam sincronismos entre si. A *Figura 6.3* mostra os gráficos, que foram utilizados para a correlação dos dados de monitorização com os de servidores e equipamentos de rede. Tendo por base a monitorização, foi possível identificar a causa direta desta situação e, posteriormente, aplicar medidas corretivas.

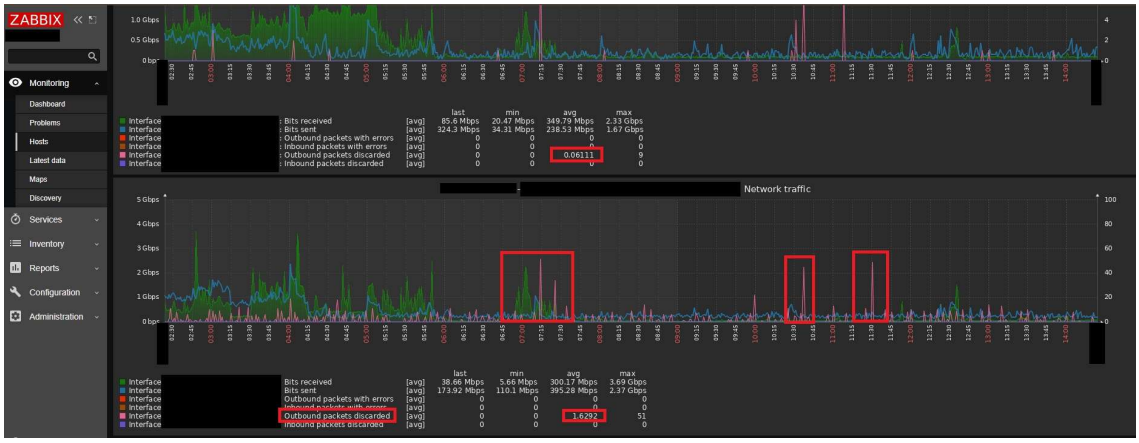

Figura 6.3: Deteção de falhas de configuração através da monitorização.

Um dos serviços fornecidos através dos *datacenters* da instituição, para todos os 265 *sites* da sua rede privativa é o serviço de *DNS* (*Domain Name System*). Com base na monitorização, foi detetada uma falha na sua arquitetura. Sempre que um administrador efetuava uma atualização no servidor *DNS*, esta atualização fazia com que tivesse impacto nos 265 *sites*, trazendo quebra de serviço no acesso à *internet*. Com base na correlação dos dados de monitorização e configuração dos *domain controllers*, identificou-se que a arquitetura em produção não possuía mecanismos de redundância. Com base nesta situação, foi desenvolvida uma nova arquitetura corretiva de *domain controllers*, para a instituição Governamental, onde se aplicou a redundância a nível da camada aplicacional e da camada física. Na *Figura 6.4* tem-se a representação dos serviços considerados críticos, que os *datacenters* da instituição disponibilizam aos seus 265 *sites*. Tendo em conta o âmbito, implementou-se servidores redundantes em *clusters* distintos, representados a vermelho e a azul, aumentando a resiliência dos serviços críticos dos 265 *sites* da instituição Governamental.

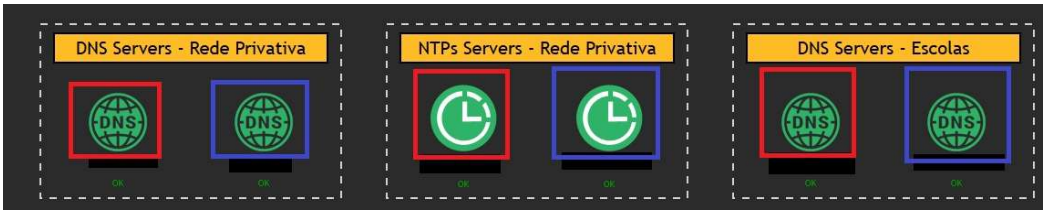

Figura 6.4: Correção dos serviços críticos para os 265 *sites* da instituição.

A monitorização dos *datacenters* fez com que se diminuísse os tempos que determinados serviços ficavam indisponíveis para a população e respetivos utilizadores ao longo dos 265 *sites* da instituição Governamental. A *Tabela 5* representa situações que comprometeram e/ou tiveram quebra de serviço, tendo por base os relatórios internos da instituição Governamental, para a população e/ou para os 265 *sites* da instituição, situações estas que tiveram como causa direta serviços dependentes da própria instituição Governamental.

Ano	Número de falhas
2021	17
2022	4
2023	3
2024	0

Tabela 5: Número de quebras de serviço, nos *datacenters* na instituição.

Apesar da evolução na monitorização dos *datacenters* da instituição Governamental, ter sido efetivamente uma melhoria na prestação de uma melhor qualidade de serviço, não só à população em geral como aos seus 265 *sites*, existe campos a refinar. Uma das situações que requer reformulação é a monitorização dos servidores de armazenamento. Devido à complexidade que estes servidores possuem, nomeadamente *clusters* independentes e mecanismos de sincronização, a monitorização precisa de todos estes é de igual modo complexa. É necessário efetuar uma monitorização deste tipo de sistemas, mais próximo do nível aplicacional, face ao tipo de informações que é obtido nestes equipamentos através da sua *MIB* não ser suficiente.

6.3. *Sites* Rede Privativa

A monitorização dos 265 *sites* da instituição Governamental encontra-se numa forma prematura, estando na maior parte dos *sites* da instituição, circunscrita apenas ao *router* que interliga à sua rede privativa. O fato do projeto de monitorização ter detetado lacunas básicas nos *sites* da instituição Governamental, nomeadamente segmentação das redes de gestão e de dados, e documentação das redes internas, tornou o processo de monitorização extremamente árduo e moroso.

O *router* de cada *site* da instituição Governamental, é monitorizado utilizando o protocolo *SNMP*. Todo o tráfego do referido *site* é, por sua vez, encaminhado através da rede privativa da instituição, para os *datacenters,* disponibilizando vários serviços internos e o acesso à *internet*. Quando existe uma falha no *router*, todos os utilizadores e equipamentos, ficam sem comunicações do *site* em questão. Deste modo, face à sua criticidade, foi aumentado a frequência das métricas de monitorização, de minuto a minuto, para trinta em trinta segundos. Esta pequena alteração teve um grande impacto na análise das métricas, no servidor *Zabbix*, devido ao fato de aumentar imenso a sua análise, face ao todo dos 265 *sites* da instituição Governamental.

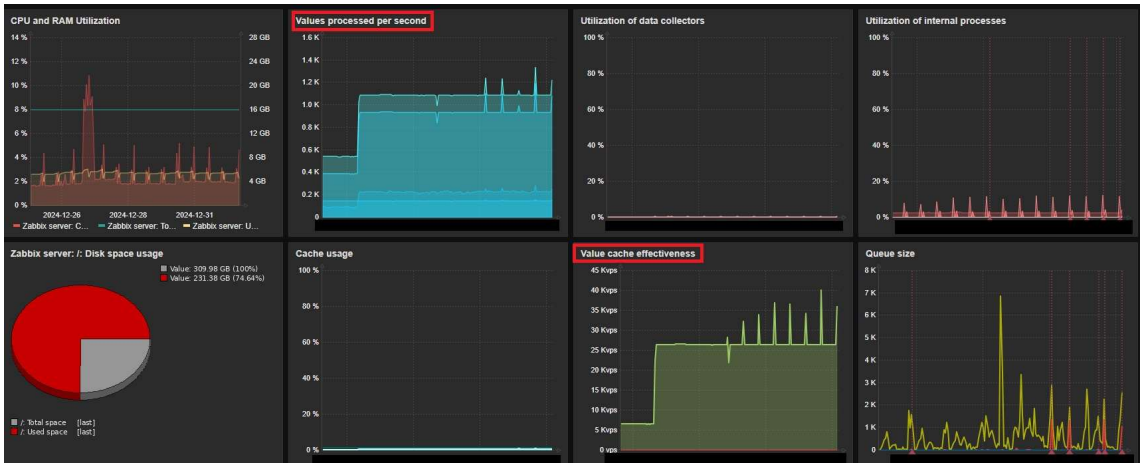

Figura 6.5: Impacto no servidor *Zabbix*, após alteração monitorização para os *sites*.

Quando esta alteração foi implementada, fez com que o servidor central de monitorização "craschasse", devido ao facto de não estar a conseguir analisar imensas métricas por segundo. Assim, foi necessário efetuar *fine tuning* na plataforma *Zabbix*, onde se teve de efetuar uma análise mais detalhada, com base no tipo de métrica obtida, classificando-a sobre que tipo de protocolo está a usar, nomeadamente *ICMP, SNMP, HTTP, HTTPS* entre outros, e tipo de dado obtido *INTEGER, FLOAT, clear text, service status.* Através desta análise, foi necessário aumentar o número de *threads* por tipo de métrica de monitorização, no servidor *Zabbix*. A *Figura 6.5,* mostra graficamente o impacto que estas alterações têm diretamente no servidor *Zabbix*, onde podemos verificar um aumento das métricas analisadas por segundo, a passar da ordem das 400 para mais de 1500.

6.4. Estrutura da Informação

A estrutura de informação implementada auxiliou os gestores de sistemas e redes no processo de análise de toda a infraestrutura e serviços da instituição Governamental. Anteriormente à monitorização através da plataforma *Zabbix*, estes efetuavam o *login* em inúmeros dispositivos e/ou portais, para saber o estado dos mesmos. Com a implementação da plataforma, estes conseguem personalizar grupos de dispositivos e/ou serviços, os quais mostram dados agregados sobre o estado destes. A *Figura 6.6* mostra na plataforma *Zabbix*, onde com base nos grupos definidos e implementados, é possível aceder à informação de cada um destes de forma mais eficiente.

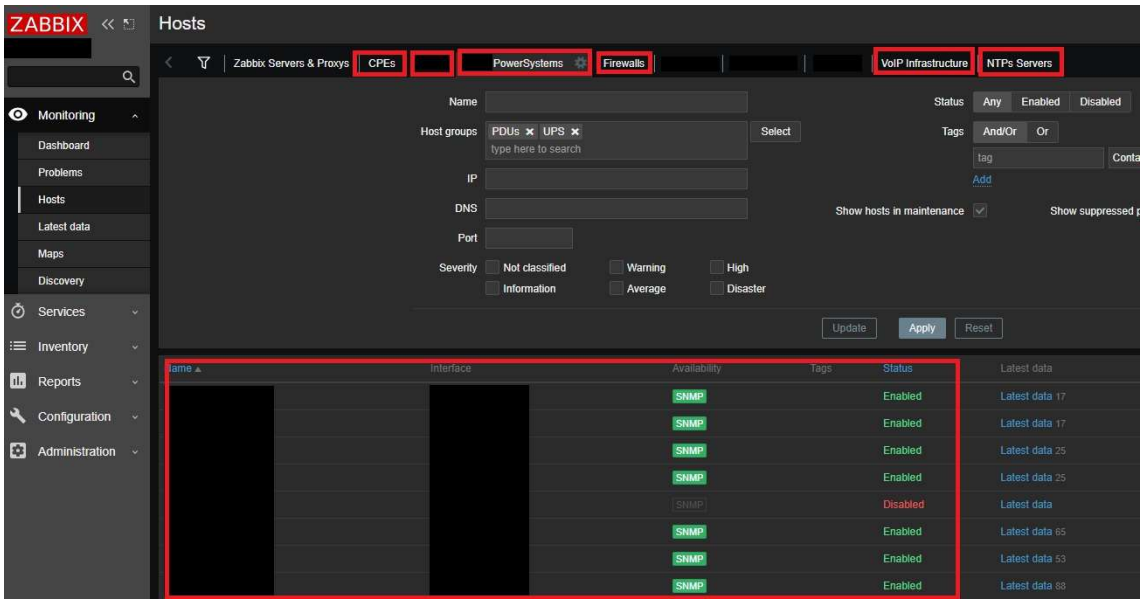

Figura 6.6: Exemplo de busca de informação baseada em grupos.

As alterações efetuadas tendo em conta a proposta arquitetural, para organização da informação, acabou por criar mais subgrupos baseados em tipo de dispositivos e serviços, para ir de encontro com as necessidades da instituição Governamental. O fato desta alteração ter sido efetuada, permitiu a instituição a partir da plataforma de monitorização, saber exatamente que dispositivos e/ou serviços possui na sua infraestrutura, podendo aplicar operações *AND* para refinar ainda mais a sua pesquisa.

Esta forma de estruturação de informação tornou benéfica para a instituição, na gestão e planeamento de recursos dos seus *datacenters* e seus 265 *sites*. Os equipamentos e/ou serviços adquiridos pela instituição nos últimos meses tiveram como base, a análise dos dados de monitorização da plataforma *Zabbix*, que auxiliou os gestores no processo de tomada de decisão.

6.5. Notificações e Alertas

O sistema de notificações e alertas implementado na instituição Governamental, permitiu possuir-se mecanismos mais céleres aquando de uma anomalia é detetada. Pelo fato de não existir anteriormente um sistema de notificações aos gestores de sistemas e redes, a sua comparação com o atual é uma evolução enorme. Numa fase inicial de implementação, as notificações enviadas pela plataforma *Zabbix* não estavam a ser refinadas, pelo que os gestores de sistemas e redes recebiam todo o tipo de notificações. Esta situação causou transtornos, pois fez com que não se desse a devida importância às notificações recebidas. Esta situação fez com que fosse necessário, reformular vários *templates* de dispositivos e serviços, e manipular determinados *triggers*, como prioritários aquando da geração de um alerta. Assim, com base nas reuniões com as equipas de sistemas e redes, o sistema de notificações passou apenas para os três níveis mais críticos da plataforma *Zabbix*.

Constatou-se que muitas das notificações recebidas são efetivamente válidas, contudo não sendo possível a sua resolução imediata, fez o que os gestores de sistemas e redes acabassem por não dar a devida atenção a este tipo de alertas. Um exemplo prático desta situação foi a geração de uma notificação de falha crítica de *hardware* de uma das UPS no *datacenter*. Devido à *UPS* ser considerado um componente crítico para o funcionamento do *datacenter*, este tipo de notificação é considerado como *disaster*, elevando a notificação para todos os gestores da instituição. Quando este tipo de situações leva meses a ser efetivamente resolvido, faz com que a monitorização existente seja negativa e prejudicial, levando com que equipas desvalorizem os sistemas de alerta. Para estas situações, é necessário existir uma tomada de decisão por parte instituição, em prol da deterioração dos sistemas de alerta às suas equipas.

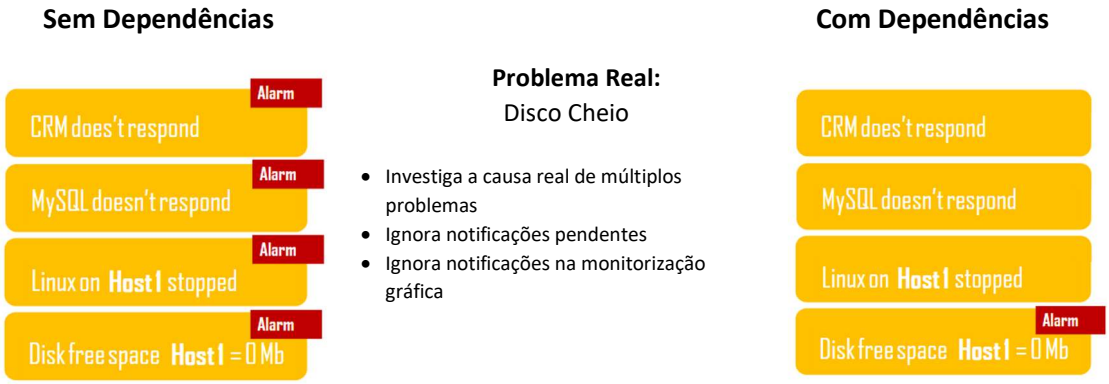

Figura 6.7: Comparação de alertas com correlação e sem correlação.

É necessário efetuar um melhor refinamento na causa dos alertas, isto é, trabalhar nos *templates* dos dispositivos e serviços, na correlação de *triggers*, permitindo desta forma um sistema de notificações mais eficiente. Esta situação irá fazer com que, os gestores de sistemas e redes sejam mais céleres a identificar a *root cause* da anomalia.

6.6. Visualização Gráfica

O grafismo elaborado na plataforma *Zabbix* permitiu às equipas de sistemas e redes possuírem de uma forma intuitiva, a noção global do funcionamento dos serviços e infraestruturas da instituição Governamental. Os mapas apresentados são dinâmicos e rotativos, auxiliando a que gestores de sistemas e redes possuam uma visão geral do funcionamento dos seus *datacenters*, *links* de acesso à *internet*, serviços críticos para seus 265 *sites* da rede privativa, entre outros mais. A *Figura 6.8* mostra a instituição Governamental a utilizar os *dashboard* criados, tendo como base informações úteis definidas pelas equipas de gestores, em ecrãs de 55 polegadas direcionados para as equipas de sistemas e redes, onde com o sistema rotativo vai alterando entre os vários *dashboards* criados.

Figura 6.8: Ecrã com a monitorização da instituição Governamental.

É necessário também aprofundar e melhorar a criação de *dashboards* automáticos, através dos próprios *templates* da plataforma *Zabbix*. Contudo, é necessário numa primeira fase, uma definição mais rigorosa, de que métricas são efetivamente necessárias para a monitorização, de maneira a evitar o desperdício de recursos, no tratamento de informação que não é relevante para os administradores.

Está em falta a apresentação de dados agregadores para superiores hierárquicos, onde de uma maneira de mais alto nível, sem muito detalhe técnico, possam analisar de forma intuitiva e saber exatamente o estado de toda a infraestrutura e serviços da instituição Governamental.

6.7. Conclusão

No que diz respeito à análise da proposta arquitetural, apesar das vantagens que uma arquitetura distribuída possui, no caso da instituição Governamental, devido à sua própria rede privativa, demostrou que o grande propósito da arquitetura distribuída não veio a trazer muito impacto na monitorização. A rede privativa da instituição Governamental faz com que todos os *sites* considerados remotos, do ponto de vista lógico, são essencialmente uma extensão das diversas *LANs* existentes, fazendo com que os pontos fulcrais de uma arquitetura distribuída não se notassem como esperado.

Apesar desta análise, confirmou-se que uma abordagem distribuída tem vantagens mesmo na situação de uma rede privativa pois, em caso de falha desta, a utilização de um *proxy* de monitorização por cada *site* remoto, faz com que não se perca as métricas de monitorização, mesmo quando não exista comunicação com o servidor central, para análise e tratamento dos dados de monitorização.

7. Conclusão

A realização desta dissertação contribui para aprofundar, compreender e aplicar conceitos fundamentais da gestão de sistemas e redes em contexto real. Foi efetuada uma análise exaustiva de toda a infraestrutura e serviços de toda a instituição Governamental, de maneira a identificar na sua essência, e as suas necessidades, que a monitorização necessitava de cobrir. A instituição Governamental teve um crescimento enorme e esperado face à evolução tecnológica, fazendo consequentemente que a sua infraestrutura se tornasse complexa e de igual modo crítica. A recente aquisição da sua própria rede privativa trouxe uma centralização de todos os serviços da instituição, e uma partilha central dos recursos a partir dos seus *datacenters*. A monitorização de todos os serviços e infraestruturas dos *datacenters* da instituição Governamental é deveras um dos pontos mais fundamentais para a monitorização, devido aos constrangimentos e consequências em caso de falha de um destes.

O estudo efetuado sobre modelos de gestão de sistemas e redes, como também de arquiteturas de monitorização centralizadas e distribuídas, veio a permitir efetuar-se uma proposta arquitetural fundamentada e coesa, com processos de comunicação bem estipulados, indo de encontro com os modelos de gestão previamente estudados. A implementação da plataforma de monitorização veio a demostrar fragilidades na instituição, que obrigou à elaboração de procedimentos internos de padronização, documentação e execução transversalmente em toda a instituição Governamental.

A implementação arquitetural teve em consideração mecanismos resilientes a falhas inclusive nos *datacenters* da instituição Governamental, face à sua criticidade na disponibilização de serviços para os seus 265 *sites.* Está em produção há mais de 3 anos e meio, com a obtenção de mais de 80 mil métricas por segundo. Trouxe uma melhoria significativa à instituição Governamental, diminuindo as quebras de serviços, e proporcionando medidas corretivas tendo por base a monitorização. A própria rede privativa da instituição Governamental veio a demostrar que a abordagem de monitorização distribuída, tal como delineada em sede de proposta arquitetural, demostrou possuir vantagens em casos muito específicos.

A implementação da plataforma de monitorização na instituição Governamental, foi considerada um sucesso, face à melhoria significativa na qualidade dos seus serviços a todos os 265 *sites*, como também no auxílio dos gestores de sistemas e redes no processo de gestão e tomada de decisão

7.1. Trabalho Futuro

Existem vários pontos deste projeto de dissertação que irão necessitar de um trabalho contínuo e permanente, como é o caso da otimização dos *templates* utilizados para monitorização dos *sites*. Esta otimização é um processo demorado, e contínuo visto ser necessário um trabalho conjunto com as equipas de manutenção e monitorização para efetuar ajustes finos, de acordo com a criticidade definida pela equipa, como também que aspetos pretendem que sejam efetivamente monitorizados.

Com as recentes atualizações da plataforma de monitorização *Zabbix*, onde em setembro de 2024 saiu versão *7.0 LTS*, existe a possibilidade de, a curto prazo, efetuar-se a atualização dos sistemas principais de monitorização, para utilização de novas *features* tais como otimização de *dashboards,* para uma maior visualização do estado dos serviços, como também novas implementações de segurança como é o caso do *TFA (Two Factor Authentication).*

Pretende-se melhorar os mecanismos atuais de visualização do estado geral da rede, de maneira que a equipa responsável pela monitorização e gestão da instituição Governamental analise de forma fácil e fluente o estado atual da rede e serviços.

Referências

[1] Z. Chen *et al.*, «A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures», *Big Data Res.*, vol. 3, pp. 10–23, abr. 2016, doi: 10.1016/j.bdr.2015.11.002.

[2] S. Kumar, S. Pallavi, e Ramyashree, «An Effective Network Monitoring Tool for Distributed Networks», em *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, out. 2020, pp. 696–700. doi: 10.1109/I-SMAC49090.2020.9243344.

[3] A. M. El-Shamy, N. A. El-Fishawy, G. Attiya, e M. A. A. Mohamed, «Anomaly Detection and Bottleneck Identification of The Distributed Application in Cloud Data Center using Software–Defined Networking», *Egypt. Inform. J.*, jan. 2021, doi: 10.1016/j.eij.2021.01.001.

[4] R. Ruel, «Desenho e implementação de uma plataforma integrada para monitorização e gestão da rede da UMa», Dissertação, Universidade da Madeira, 2016.

[5] K. Barker e S. Morris, *CCNA security 640-554 official cert guide*. Indianapolis, IN: CISCO Press, 2013.

[6] M. Brattstrom e P. Morreale, «Scalable Agentless Cloud Network Monitoring», em *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, jun. 2017, pp. 171–176. doi: 10.1109/CSCloud.2017.11.

[7] Cisco Systems Inc, Ed., *Internetworking technologies handbook*, 4. ed. Indianapolis, Ind: Cisco Press, 2004.

[8] H. Zimmermann, «OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection», *IEEE Trans. Commun.*, vol. 28, n.º 4, pp. 425–432, abr. 1980, doi: 10.1109/TCOM.1980.1094702.

[9] de S. Sebastião, «Building a Network Operations Center (NOC) Solution». Master in Informatic Engineering, fevereiro de 2016.

[10] E. Benetti, M. Fracassetti, e G. Mazzini, «Case study for Data Center Distributed Monitoring», em *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, jan. 2022, pp. 0248–0253. doi: 10.1109/CCWC54503.2022.9720814.

[11] S. M. M. T. Moreira, «Monitorização de Redes e Sistemas Informáticos», out. 2014, Acedido: 6 de setembro de 2021. [Em linha]. Disponível em: https://repositorio-aberto.up.pt/handle/10216/76912

[12] R. White e D. Donohue, *The art of network architecture*. Indianapolis, Indiana: Cisco Press, 2014.

[13] Y. Yemini, «The OSI network management model», *Commun. Mag. IEEE*, vol. 31, pp. 20–29, jun. 1993, doi: 10.1109/35.212418.

[14] A. Clemm, *Network management fundamentals: a guide to understanding how network management technology really works*. Indianapolis, Ind: Cisco Press, 2007.

[15] P. Goyal, R. Mikkilineni, e M. Ganti, «FCAPS in the Business Services Fabric Model», em *2009 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*, jun. 2009, pp. 45–51. doi: 10.1109/WETICE.2009.21.

[16] A. Gorod, R. Gove, B. Sauser, e J. Boardman, «System of Systems Management: A Network Management Approach», em *2007 IEEE International Conference on System of Systems Engineering*, abr. 2007, pp. 1–5. doi: 10.1109/SYSOSE.2007.4304218.

[17] E. Monteiro e F. Boavida, *Engenharia de Redes Informáticas, 10ª edição Actualizada e Aumentada*. 2011.

[18] E. Marques, «Interoperabilidade e Otimização da Gestão de Redes com a Framework NSDL», Universidade da Madeira, 2013.
[19] 14:00-17:00, «ISO/IEC 7498-4:1989», ISO. Acedido: 9 de julho de 2024. [Em linha]. Disponível em: https://www.iso.org/standard/14258.html
[20] «End System to Intermediate System Routing Exchange Protocol for use in conjunction with ISO 8473», n.º 995. em Request for Comments. RFC Editor, 1 de abril de 1986. [Em linha]. Disponível em: https://www.rfc-editor.org/info/rfc995
[21] R. M. Oviedo, F. Ramos, S. Gormus, P. Kulkarni, e M. Sooriyabandara, «A Comparison of Centralized and Distributed Monitoring Architectures in the Smart Grid», *IEEE Syst. J.*, vol. 7, n.º 4, pp. 832–844, dez. 2013, doi: 10.1109/JSYST.2013.2246033.
[22] V. Jarlow, «SERVER HARDWARE HEALTH STATUS MONITORING», Dissertação, University of Skovde, 2018.
[23] K. Alhamazani *et al.*, «An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art», *Computing*, vol. 97, n.º 4, pp. 357–377, abr. 2015, doi: 10.1007/s00607-014-0398-5.
[24] N. Dimonte, «Centralized Monitoring Infrastructure on Cloud: An Open Source Approach.», laurea, Politecnico di Torino, 2024. Acedido: 7 de agosto de 2024. [Em linha]. Disponível em: https://webthesis.biblio.polito.it/30849/
[25] C. Wang, K. Schwan, V. Talwar, G. Eisenhauer, L. Hu, e M. Wolf, «A flexible architecture integrating monitoring and analytics for managing large-scale data centers», em *Proceedings of the 8th ACM international conference on Autonomic computing*, Karlsruhe Germany: ACM, jun. 2011, pp. 141–150. doi: 10.1145/1998582.1998605.
[26] X. Li, K. Li, Y. Ding, D. Wei, e X. Ma, «Application of Autonomous Monitoring Method Based on Distributed Environment Deployment in Network Fault», *J. Phys. Conf. Ser.*, vol. 1486, n.º 2, p. 022048, abr. 2020, doi: 10.1088/1742-6596/1486/2/022048.
[27] J. Spring, «Monitoring Cloud Computing by Layer, Part 2», *IEEE Secur. Priv.*, vol. 9, n.º 3, pp. 52–55, mai. 2011, doi: 10.1109/MSP.2011.57.
[28] I. Ghafir, V. Prenosil, J. Svoboda, e M. Hammoudeh, «A Survey on Network Security Monitoring Systems», em *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, ago. 2016, pp. 77–82. doi: 10.1109/W-FiCloud.2016.30.
[29] X. Zhang, H. Du, J. Chen, Y. Lin, e L. Zeng, «Ensure Data Security in Cloud Storage», em *2011 International Conference on Network Computing and Information Security*, mai. 2011, pp. 284–287. doi: 10.1109/NCIS.2011.64.
[30] L. Elsen, F. Kohn, C. Decker, e R. Wattenhofer, «goProbe: a scalable distributed network monitoring solution», em *2015 IEEE International Conference on Peer-to-Peer Computing (P2P)*, set. 2015, pp. 1–10. doi: 10.1109/P2P.2015.7328518.
[31] A. Roy *et al.*, «Cloud Datacenter SDN Monitoring: Experiences and Challenges», em *Proceedings of the Internet Measurement Conference 2018*, Boston MA USA: ACM, out. 2018, pp. 464–470. doi: 10.1145/3278532.3278572.
[32] A. Petitti *et al.*, «A distributed heterogeneous sensor network for tracking and monitoring», em *2013 10th IEEE International Conference on Advanced Video and Signal Based Surveillance*, ago. 2013, pp. 426–431. doi: 10.1109/AVSS.2013.6636677.
[33] T. M. Chen e S. S. Liu, «A model and evaluation of distributed network management approaches», *IEEE J. Sel. Areas Commun.*, vol. 20, n.º 4, pp. 850–857, mai. 2002, doi: 10.1109/JSAC.2002.1003049.
[34] Voronezh State Technical University, Voronezh, Russian Federation *et al.*, «Designing the architecture of a distributed system for information monitoring of IoT and IIoT infrastructures traffic», *Int. J. Inf. Technol. Secur.*, vol. 16, n.º 1, pp. 49–56, mar. 2024, doi: 10.59035/BTBI7690.
[35] D. Thummar, I. Nawab, e S. G. Kulkarni, «Distributed In-band Network Telemetry», em *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing*

Workshops (CCGridW), mai. 2023, pp. 287–289. doi: 10.1109/CCGridW59191.2023.00060.

[36] S. Saha e A. Majumdar, «Data centre temperature monitoring with ESP8266 based Wireless Sensor Network and cloud based dashboard with real time alert system», em *2017 Devices for Integrated Circuit (DevIC)*, mar. 2017, pp. 307–310. doi: 10.1109/DEVIC.2017.8073958.

[37] D.-G. Akestoridis e P. Tague, «HiveGuard: A Network Security Monitoring Architecture for Zigbee Networks», em *2021 IEEE Conference on Communications and Network Security (CNS)*, out. 2021, pp. 209–217. doi: 10.1109/CNS53000.2021.9705043.

[38] E. I. Papagiannakopoulou *et al.*, «A privacy-aware access control model for distributed network monitoring», *Comput. Electr. Eng.*, vol. 39, n.º 7, pp. 2263–2281, out. 2013, doi: 10.1016/j.compeleceng.2012.08.003.

[39] N. Van Tu, J. Hyun, e J. W.-K. Hong, «Towards ONOS-based SDN monitoring using in-band network telemetry», em *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, set. 2017, pp. 76–81. doi: 10.1109/APNOMS.2017.8094182.

[40] M. H. Kim, S.-H. Lim, e J.-G. Kim, «Modeling of a real-time distributed network management based on TMN and the TMO model», em *Proceedings of the Eighth International Workshop on Object-Oriented Real-Time Dependable Systems, 2003. (WORDS 2003).*, jan. 2003, pp. 56–63. doi: 10.1109/WORDS.2003.1218066.

[41] R. Akhter e S. A. Sofi, «Precision agriculture using IoT data analytics and machine learning», *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, n.º 8, Part B, pp. 5602–5618, set. 2022, doi: 10.1016/j.jksuci.2021.05.013.

[42] Prometheus, «Overview: What is Prometheus?» Acedido: 10 de março de 2025. [Em linha]. Disponível em: https://prometheus.io/docs/introduction/overview/

[43] «Nagios Architecture Overview». Acedido: 10 de março de 2025. [Em linha]. Disponível em: https://support.nagios.com/kb/article/nagios-xi-architecture-overview-35.html

[44] L. Marote, «Monitorização de uma Rede de Média Dimensão com Plataforma Open-Source», Universidade da Madeira, Funchal, Projeto de Licenciatura em Engenharia Informática, jul. 2020.

Anexos

Anexo A – Procedimento de Instalação *Zabbix*

```
# Procedimento Instalação Zabbix Server 6.0-LTS (Debian 11 Bullseye)
# Procedimento Desenvolvido por Lisandro Marote
# Version 1.0 (25/11/2021)

# Atualizar os repositórios do LXC Container
apt update
apt upgrade
dpkg-reconfigure tzdata

# Instalar PHP 7.4
# Não instalar PHP 8.0 ou 8.1, zabbix crasha com estas versões.
apt install libapache2-mod-php7.4
apt install php7.4-fpm
apt install php7.4-cgi
apt install php7.4-common

# Actualizar os repositórios do LXC Container
apt update
apt upgrade

# Instalar PHP 7.4
apt install php7.4

# Instalação de mais bibliotecas do PHP (necessárias para o Zabbix
Server)
apt-get install php7.4-
{fpm,bcmath,bz2,intl,gd,mbstring,mysql,zip,curl,ldap,xml}

# Instalação e Ativação do Módulo Apache
apt install apache2
systemctl start apache2
systemctl enable apache2
systemctl restart apache2

# Verificar o estado o serviço
systemctl status apache2.service

# Adição dos Repositórios e instalação MariaDB 10.6 Stable (Utilizar
os repositórios do Porto, os de Lisboa possuem problemas)
apt-get install software-properties-common dirmngr apt-transport-https
# Importar as keys do MariaDB
apt-key adv --fetch-keys
'https://mariadb.org/mariadb_release_signing_key.asc'
# Adicionar o repositório para futuras atualizações (este passo poderá
ser realizado doutra forma, adicionando na directoria
/etc/apt/sources.list.d)
add-apt-repository 'deb [arch=amd64,i386,arm64,ppc64el]
https://mirrors.up.pt/pub/mariadb/repo/10.6/debian bullseye main'
apt update
apt upgrade

# Instalar MariaDB server
apt-get install mariadb-server

# Fazer o procedimento de instalação "segura" do MariaDB server
```

```
mysql_secure_installation

# Dar enable ao serviço aquando a máquina arrancar
systemctl enable mariadb

# Forma alternativa de configurar as actualizações do MariaDB server:
# Editar o ficheiro sources.list e comentar com "#" o repositório da
MariaDB server
nano /etc/apt/sources.list
    #deb [arch=i386,ppc64el,arm64,amd64]
https://mirrors.up.pt/pub/mariadb/repo/10.6/deb>
    #deb-src [arch=i386,ppc64el,arm64,amd64]
https://mirrors.up.pt/pub/mariadb/repo/10.6>

# Criar um ficheiro 'MariaDB.list' no directório
/etc/apt/source.list.d/
cd /etc/apt/sources.list.d/
touch MariaDB.list

# Adicionar o seguinte dentro do ficheiro 'MariaDB.list'
nano MariaDB.list
    # MariaDB 10.6 repository list - created 2021-11-25 08:30 UTC
    # https://mariadb.org/download/
    deb [arch=amd64,i386,arm64,ppc64el]
https://mirrors.up.pt/pub/mariadb/repo/10.6/debian bullseye main
    deb-src https://mirrors.up.pt/pub/mariadb/repo/10.6/debian
bullseye main


# Criação duma base de dados 'datazabbix' para o utilizador
'adminzabbix' com a password 'Ursinho2022@'
mysql -u root -p
DebianUpdate1024@

create database datazabbix character set utf8mb4 collate utf8mb4_bin;
create user adminzabbix@localhost identified by 'Ursinho2022@';
grant all privileges on datazabbix.* to adminzabbix@localhost;
flush privileges;
quit;

# Obter os repositórios mais recentes do Zabbix 6.0-LTS
wget https://repo.zabbix.com/zabbix/5.0/debian/pool/main/z/zabbix-
release/zabbix-release_5.0-1%2Bbullseye_all.deb
dpkg -i zabbix-release_5.0-1+bullseye_all.deb
apt update
apt upgrade

# Instalaçãp do Zabbix server, Agent e Zabbix frontend
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
zabbix-sql-scripts zabbix-agent
systemctl restart apache2

# Importar para a base de dados os ficheiros do Zabbix
zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -u
adminzabbix -p datazabbix
Ursinho2022@

# Editar o ficheiro zabbix_server.conf e colocar de acordo com a base
de dados
nano /etc/zabbix/zabbix_server.conf
DBHost=localhost
```

```
DBName=datazabbix
DBUser=adminzabbix
DBPassword=Ursinho2022@

# Reiniciar e ativar os seguintes serviços
systemctl restart zabbix-server zabbix-agent apache2
systemctl enable zabbix-server zabbix-agent apache2

# Editar ficheiro de configuração do PHP e colocar como se segue:
nano /etc/php/7.4/apache2/php.ini
[Date]
; http://php.net/date.timezone
date.timezone =Europe/Lisbon

post_max_size = 32M
max_execution_time = 300
max_input_time = 300
memory_limit = 256

# Editar o ficheiro do zabbix apache e tirar de comentário
data.timezone
nano /etc/zabbix/apache.conf
php_value max_execution_time 300
php_value memory_limit 256M
php_value post_max_size 32M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value max_input_vars 10000
php_value always_populate_raw_post_data -1
php_value date.timezone Europe/Lisbon

# Iniciar os Seviços Zabbix Server e Agent, e ativar estes no arranque
do sistema
systemctl start zabbix-server zabbix-agent
systemctl enable zabbix-server zabbix-agent
systemctl restart apache2

# Abrir o Browser e iniciar o processo de conclusão do Zabbix 6.0 da
seguinte forma:
https://IP_da_máquina/zabbix
```

Anexo B – Instalação Módulo *SSL Zabbix server*

```
# Colocação de um SelfCertificated no Zabbix Server
# Procedimento Desenvolvido por Lisandro Marote
# Version 2.2 (01/12/2021)

# Criar o Diretório para Armazenar as Chaves com as Permissões
Corretas
mkdir -p /etc/apache2/ssl/private
chmod 700 /etc/apache2/ssl/private

# Gerar o Certificado e Chave para o Frontend Apache
openssl req -x509 -nodes -days 3650 -newkey rsa:4096 -keyout
/etc/apache2/ssl/private/zabbix_VLAN1.key -out
/etc/apache2/ssl/zabbix_VLAN1.crt

# Editar o Ficheiro do apache2/ssl/apache-selfsigned
cp /etc/apache2/sites-available/default-ssl.conf zabbix-https-
VLAN1.conf
nano /etc/apache2/sites-available/zabbix-https-VLAN1.conf

<VirtualHost 10.1.222.246:443>
                DocumentRoot /usr/share/zabbix
                ServerName 10.2.4.1
                SSLCertificateFile /etc/apache2/ssl/apache-
selfsigned.crt
                SSLCertificateKeyFile /etc/apache2/ssl/private/apache-
selfsigned.key
</VirtualHost>

# Ativar o Apache HTTPS e ativar o seu módulo
a2ensite zabbix-https-VLAN1.conf
a2enmod ssl
a2enmod rewrite
systemctl reload apache2.service

# Configurações avançadas de segurança (Para o utilizador não ver
dados acerca do Servidor de apache aquando ocorre um 404 na página)
nano /etc/apache2/conf-available/security.conf
ServerSignature Off
ServerTokens Prod
# (Versão 7.4 por defeito já trás esta definição desativa)
nano /etc/php/7.4/apache2/php.ini
expose_php = Off

# Boa Prática de Segurança para o Zabbix
nano /etc/apache2/conf-available/zabbix.conf
<IfModule mod_alias.c>
    Alias /UMazabbix /usr/share/zabbix
</IfModule>

# Remover o Ficheiro index.html
rm /var/www/html/index.html

# Reiniciar todos os Serviços e verificar o seu status
systemctl restart apache2
systemctl restart zabbix-server
systemctl restart zabbix-agent
```

Anexo C – Encriptação Comunicações com *Zabbix server*

```
# Encriptação dados enviados entre Host (Zabbix-Agent) e o Zabbix
Server
# Procedimento Desenvolvido por Lisandro Marote
# Version 1.1 (13/10/2020)

# Criar uma pasta 'zabbix' no directório /home/zabbix
cd
cd /home
mkdir zabbix
cd zabbix

# Criar a chave .psk
# Copiar a Key gerada que foi gravada no ficheiro secret.psk
openssl rand -hex 32 > secret.psk

# Atribuir os privilégios ao utilizador zabbix
chown zabbix:zabbix secret.psk
chmod 640 secret.psk

# Editar as configurações do Zabbix-Agent
nano /etc/zabbix/zabbix_agentd.conf

# Colocar os parametros tal como se segue
TLSConnect=psk
TLSAccept=psk
TLSPSKIdentity=Paladino_Encryption
TLSPSKFile=/home/zabbix/secret.psk

# Reinicar o serviço Zabbix-agent
systemctl restart zabbix-agent

# Na GUI do Zabbix Server, dirigir-se às configurações do host
clicar no host -> Encrpyption

# Colocar as configurações da seguinte forma:
Conections to host:     PSK
Conections from host:   PSK

PSK identity:           Paladino_Encryption
PSK:
d6ea2ac4e07897262abce384931f324a03d4e71aa35fa49afc46588b1788ac06
```

Anexo D – Procedimento Monitorização *LXC Container*

```
# Procedimento Instalação Zabbix-Agent 5.0-LTS em LXC Containeres
(Debian10 buster)
# Procedimento Desenvolvido por Lisandro Marote
# Version 3.2 (16/09/2021)

# Adicionar os repositórios do Zabbix mais recente na máquina
wget https://repo.zabbix.com/zabbix/5.0/debian/pool/main/z/zabbix-
release/zabbix-release_5.0-1%2Bbuster_all.deb
dpkg -i zabbix-release_5.0-1+buster_all.deb
apt update

# Instalação do Zabbix Agent na Máquina
apt-get install zabbix-agent

# Editar o Ficheiro de Configuração do Zabbix Agent e colocar os
Parâmetros do Zabbix Server
# ***************** NOTA IMPORTANTE *****************
# Dependendo da VLAN onde está o Dispositivo Colocar o IP do Zabbix
Server que se enquadra:
#   VLAN 1 (Docentes):  10.1.222.246
#   VLAN 2 (Alunos):    10.2.42.16
# ***************** *****************
nano /etc/zabbix/zabbix_agentd.conf
Server=10.2.4.6
ServerActive=10.2.4.6
Hostname=Container_Hostname

# Criar o ficheiro 'UserParameter_LXC.conf' no directório
/etc/zabbix/zabbix_agentd.d/UserParameter_LXC.conf
# Este ficheiro irá permitir a recolha das métricas como CPU,RAM e
Swap corretas a partir dum LXC Container.
cd /etc/zabbix/zabbix_agentd.d/
touch UserParameter_LXC.conf
nano UserParameter_LXC.conf

# Colar dentro do ficheiro 'UserParameter_LXC.conf' o seguinte:

    # User Parameter for LXC Containers
    # Developed by Lisandro Marote
    # Version 3.2 (16/09/2021)
    UserParameter=ct.memory.size[*],free -b | awk '$ 1 == "Mem:"
{total=$ 2; used=$ 3; pused=(($ 3*100)/$ 2); free=$ 4; shared=$ 5;
buffers=$ 6; available=$ 7; if("$1" == "") {printf("%.0f", total )}
else {printf("%.0f", $1 "" )} }'
    UserParameter=ct.swap.size[*],free -b | awk '$ 1 == "Swap:"
{total=$ 2; used=$ 3; free=$ 4; pfree=($ 4*100/$ 2); pused=($ 3*100/$
2); if("$1" == "") {printf("%.0f", free )} else {printf("%.0f", $1 ""
)} }'
    UserParameter=ct.cpu.num[*],nproc
    UserParameter=ct.reboottime[*],uptime
    UserParameter=ct.lastboot[*],who -b
    UserParameter=ct.uptime[*],uptime -p
    UserParameter=ct.datatime[*],date '+%s'
    UserParameter=ct.operatingsystem[*],cat /etc/os-release

# Ligar o Serviço Zabbix Agent e dar Enable aquando a Máquina se Ligar
service zabbix-agent start
```

```
systemctl enable zabbix-agent
systemctl restart zabbix-agent.service
```

Anexo E – Procedimento Monitorização *Website*

```
# Procedimento para monitorização
# Procedimento Desenvolvido por Lisandro Marote
# Version 1.3 (06/04/2022)

# Criar uma pasta 'zabbix' no directório /home/zabbix
cd
cd /home
mkdir zabbix
cd zabbix

# Criar o script 'checkssl.sh'
# Editar e colar o script baseado na biblioteca openssl
touch checkssl.sh
nano checkssl.sh

    data=`echo | openssl s_client -servername $1 -connect $1:${2:-443}
2>/dev/null | openssl x509 -noout -enddate | sed -e 's#notAfter=##'`
    ssldate=`date -d "${data}" '+%s'`
    nowdate=`date '+%s'`
    diff="$((${ssldate}-${nowdate}))"
    echo $((${diff}/86400))


# Atribuir os privilégios ao utilizador zabbix de execução
chown zabbix:zabbix checkssl.sh
chmod a+x checkssl.sh

# Para testar o funcionamento do scrip basta fazer o seguinte:
./checkssl.sh uma.pt

# Editar as configurações do Zabbix-Agent
nano /etc/zabbix/zabbix_agentd.conf

# Colocar os parametros tal como se segue
AllowKey=system.run[/home/zabbix/checkssl.sh *]
Server=127.0.0.1,
IP_DO_ZABBIX_SERVER_OU_ZABBIX_PROXY___O_IP_DE_LOCALHOST_TEM_DE_ESTAR_O
BRIGATORIAMENTE

# Reinicar o serviço Zabbix-agent
systemctl restart zabbix-agent

# Na GUI do Zabbix Server, dirigir-se às configurações do host
Host name       O nome do Website sem qualquer HTTPs (Exemplo: uma.pt)
Interfaces      Agent       127.0.0.1

# Dirigir-se à TAB 'Macros' e adicionar as duas Macros:
{$SITE_STRING}          Value: "universidade"
UMA_PARTE_DA_STRING_QUE_SE_APANHA_DO_FRONTEND_DO_WEBSITE (Exemplo:
universidade)
{$SITE_URL}             Value:  "uma.pt"
O_WEBSITE_SEM_HTTPS_SOMENTE_O_NOME_MAIS_SECO

# Dirigir-se à TAB 'Templates' e adicionar o seguinte:
Template Web-Monitoring
```

```
# Se a monitorização de onde vai ser executado o agent tem encriptção
é necessário configurar.
# Na GUI do Zabbix Server, dirigir-se às configurações do host
clicar no host -> Encrpyption

# Colocar as configurações da seguinte forma:
Conections to host:     PSK
Conections from host:   PSK

PSK identity:           Paladino_Encryption
PSK:
d6ea2ac4e07897262abce384931f324a03d4e71aa35fa49afc46588b1788ac06
```