FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Anderson Almeida Pedroso

MONITORAMENTO DE ATIVOS DE REDE UTILIZANDO A FERRAMENTA PRTG NETWORK MONITOR

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Anderson Almeida Pedroso

MONITORAMENTO DE ATIVOS DE REDE UTILIZANDO A FERRAMENTA PRTG NETWORK MONITOR

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação do Prof. Esp. Rogério Nunes de Freitas.
Área de concentração: Segurança da Informação

Americana, S. P.

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Pedroso, Anderson Almeida
P415m Monitoramento de ativos de rede utilizando a ferramenta PRTG network monitor. / Anderson Almeida Pedroso. – Americana: 2016.
58f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Rogério Nunes de Freitas

1. Redes de computadores 2.Segurança em sistemas de informação I. Freitas, Rogério Nunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519
681.518.5

Anderson Almeida Pedroso

MONITORAMENTO DE ATIVOS DE REDE UTILIZANDO A FERRAMENTA PRTG NETWORK MONITOR

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 20 de mês de defesa da banca de 2016.

Banca Examinadora:

Rogério Nunes de Freitas (Presidente)
Especialista
Faculdade de Tecnologia de Americana

Benedito Aparecido Cruz (Membro)
Graduado
Faculdade de Tecnologia de Americana

Renato Kraide Sofnner (Membro)
Doutor
Faculdade de Tecnologia de Americana

Faculdade de Tecnologia de Americana

TERMO DE AUTORIZAÇÃO PARA DIVULGAÇÃO DE INFORMAÇÕES DE EMPRESAS

Empresa: Padtec S/A

CNPJ: 03.549.807-0001/76 **Inscrição Estadual:** 244.661.040.111

Endereço completo: Rua Doutor Ricardo Benetton Martins, s/n, Polo II de Alta Tecnologia, Campinas, São Paulo – CEP: 13086-510

Representante da empresa: Gustavo Carmelindo Peron

Telefone: (19) 2104-9700 **e-mail:** gustavo.peron@padtec.com.br

Tipo de produção intelectual: (X) TCC[1] ( ) TCCE[2] ( ) Dissertação ( ) Tese

Título/subtítulo: MONITORAMENTO DE ATIVOS DE REDE UTILIZANDO A FERRAMENTA PRTG NETWORK MONITOR

Autor[3]: Anderson Almeida Pedroso **RA[3]:** 0040451121003

Orientador: Rogério Nunes de Freitas

Curso/Programa de Pós-graduação: Segurança da Informação

Como representante da empresa acima nominada, declaro que as informações e/ou documentos disponibilizados pela empresa para o trabalho citado:

(X) Podem ser publicados sem restrição.

( ) Possuem restrição parcial por um período[4] de _____ anos, não podendo ser publicadas as seguintes informações e/ou documentos: _____

( ) Possuem restrição total para publicação por um período[4] de _____ anos, pelos seguintes motivos: _____

03.549.807/0001-76
PADTEC S/A.
Rua Dr. Ricardo Benetton Martins, s/nº
Pq. II do Polo de Alta Tecnologia - CEP 13086-902
CAMPINAS - SP

Representante da empresa

Campinas, 31 de Maio de 2016
Local e Data

[1] TCC – monografia de Curso de Graduação.
[2] TCCE – monografia de Curso de Especialização.
[3] Para os trabalhos realizados por mais de um aluno, devem ser apresentados os dados de todos os alunos.
[4] O período de restrição parcial ou total deste Termo deve ser igual ao período definido em termo específico estabelecido entre a Fatec Americana e a empresa. A íntegra do resumo e os metadados ficarão disponibilizados.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, por ter me dado força para concluir este trabalho, ao meu orientador Rogério Nunes de Freitas, a empresa em que trabalho Padtec S/A, a minha esposa Ana Paula e a todos os meus familiares, e todos os professores da Fatec pelo conhecimento e dedicação durantes esses anos.

DEDICATÓRIA

Ao meu tio Israel Rodrigues Pedroso e minha esposa Ana Paula Borges, que sempre me ajudaram nessa trajetória.

RESUMO

Com a grande evolução das redes de computadores nas empresas de todos os portes, e a integração com um vasto número de ativos de rede, tais como computadores, servidores, nobreaks, switches, firewalls, impressoras, entre outros dispositivos, fez com que o gerenciamento destas redes necessitasse de uma ferramenta para monitorar e controlar estes dispositivos e aplicações. Existe uma evolução muito importante nunca visto antes, tornando estes dispositivos como parte crucial de uma organização, que deseja chegar a um determinado padrão de segmento global da tecnologia. Atualmente o mercado disponibiliza várias soluções de gerenciamento de redes como: PRTG Network Monitor, Zabbix, Nagios, Cacti, Zenoss, MRTG, e outras soluções. Todas com o âmbito de ajudar os administradores a garantirem o bom funcionamento das redes e aplicações. Por esse motivo, antes de escolher qual ferramenta utilizar, é necessário um longo período de estudos e testes, para só assim poder identificar quais destas incorporam funcionalidades fundamentais para um gerenciamento confiável, seguro e eficiente. O presente trabalho apresenta de maneira simples e objetiva a ferramenta de gerência de redes PRTG Network Monitor, como uma plataforma completa e unificada para monitoração de redes, incluindo seus dispositivos e aplicações.
Este projeto exibe como uma rede gerenciada ajuda uma organização a ter meios para evitar que os seus dispositivos de redes não causem prejuízo, caso haja alguma parada inesperada seja ela física ou lógica.

Palavras Chave: Monitoramento de Redes; PRTG; Gerência de Redes.

ABSTRACT

With the great development of computer networks in companies of all sizes, and integration with a wide range of network assets, such as computers, servers, nobreaks, switches, firewalls, printers, and other devices, has made the management these networks needed a tool for monitoring and controlling these devices and applications. There is a very important development never seen before, making these devices as a crucial part of an organization, you want to reach a certain standard of global technology segment. Currently the market offers several network management solutions such as PRTG Network Monitor, Zabbix, Nagios, Cacti, Zenoss, MRTG, and other solutions. All with the scope to help directors to ensure the smooth operation of networks and applications. Therefore, before choosing which tool to use, a long period of research and testing is needed to just so you can identify which of these incorporate key features for a reliable, safe and efficient management. This paper presents a simple and objective way to network management tool PRTG Network Monitor, as a complete and unified platform for monitoring networks, including its features and applications.

This project shows how a managed network helps an organization to have means to prevent their network devices do not cause damage, if any unexpected stop whether physical or logical..

Keywords: *Network monitoring; PRTG; Network Management.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SÍMBOLOS E SIGLAS

CPU	*Central Processing Unit*
FTP	*File Transfer Protocol*
GB	*Gigabyte*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
MB	*Megabyte*
MBPS	*Megabits Per Second*
MIB	*Management Information Base*
PDU	*Protocol Data Unit*
RAM	*Random Access Memory*
SMI	*Structure of Management Information*
SMS	*Short Message Service*
SNMP	*Simple Network Management Protocol*
TCP	*Transfer Control Protocol*
TI	Tecnologia da Informação
UDP	*User Datagram Protocol*
UPS	*Unit Power Supply*
WMI	*Windows Management Instrumentation*

1 INTRODUÇÃO

O objetivo da gerência de redes é monitorar e controlar os elementos da rede seja eles físicos ou lógicos, assegurando certo nível de qualidade de serviço. Para realizar esta tarefa, os administradores de redes são geralmente auxiliados por um sistema capaz de gerenciar dispositivos de redes e aplicações.

Um sistema de gerência de rede pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle.

Este sistema oferece uma interface única, com informações sobre a rede e pode oferecer um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede (LOPES, 2010).

Com tantos ativos, que são partes da rede de uma organização, existe a grande preocupação com a interrupção desses é necessária a devida atenção do time de tecnologia da informação, para que esteja precavido e dê a solução o mais rápido possível.

O desenvolvimento deste trabalho está diretamente ligado aos três pilares de segurança da informação, e a partir deste princípio pode-se definir que os sistemas de gerenciamento desses dispositivos se tornaram uma aplicação importante em redes de computadores, pois seu principal objetivo é fazer com que os pilares funcionem em sinergia evitando riscos ao negócio.

O escopo para este trabalho foi apresentar uma das soluções disponíveis para se gerenciar uma rede, utilizando a aplicação PRTG Network Monitor em um ambiente corporativo, explicando quais são as vantagens e desvantagens que esta aplicação tem em relação a sua utilização.

A **problemática** deu-se ao entorno da análise de custo benefício, onde foi necessário definir se a aplicação PRTG é uma opção com mais vantagens em relação às outras aplicações existentes, para o gerenciamento de ativos de redes e com isso responder à pergunta: Com relação ao custo-benefício para a implantação desta aplicação, torna-o uma ferramenta viável para um ambiente corporativo?

O **objetivo** geral deste projeto foi analisar se, uma ferramenta de monitoramento de rede traz benefícios a uma organização, relatando suas vantagens e desvantagens.

Como objetivos específicos foram definidos os seguintes pontos:

a) Conhecer todo o processo e as características da aplicação de monitoramento de redes.
b) Fazer testes mostrando as vantagens de se ter uma rede monitorada.
c) Mostrar os diversos tipos de monitoramento para dispositivos de rede.
d) Ser feito um estudo dos resultados obtidos, mostrando a eficiência da aplicação estudada.

Como **justificativa**, a escolha deste tema teve como enfoque principal ajudar os administradores de redes, a ter controle de seus dispositivos, levando em consideração o grande acréscimo de equipamentos que utilizam a rede local de uma organização. Com este aumento expressivo, quanto mais equipamentos conectados, maior será a chance de algum deles sofrer falhas podendo causar um amplo risco aos negócios.

Como **método**, toda a pesquisa foi realizada com procedimentos técnicos, e de modo experimental, exibindo exemplos reais e seus resultados, que foram realizados dentro de um ambiente corporativo, onde gerou o conteúdo deste projeto.

A técnica utilizada foi observar os ativos de rede de uma organização e analisar o conteúdo gerado pela aplicação, relatando todos os dados obtidos neste trabalho. Com base nestes dados foi avaliada a grande utilidade de se ter uma aplicação de gerência de redes, que foi claramente registrado ao longo deste trabalho, utilizando o procedimento bibliográfico e documental.

As **hipóteses** principais para este estudo e pesquisa foram:

a) Verificar se o PRTG se mostrou uma aplicação, com fácil instalação e com uma interface simples de operar, sem a necessidade de ter um hardware de última geração para o bom funcionamento, mesmo que isso não signifique uma vantagem real.

b) Sabendo que existem diversas aplicações com o mesmo propósito e com mais tempo de mercado. E que muitos administradores de redes utilizam sem nem um tipo de custo, é necessário averiguar se outras aplicações apresentam vantagens e características que não justifiquem a relação de um com o outro.
c) O que o PRTG Network Monitor tem de melhor, em relação às outras aplicações. Uma das melhores ferramentas de relatórios, gráficos, sensores e fácil interação.

Como principais fontes de pesquisa bibliográfica, este projeto tem como referência bibliográfica autores renomados da área de segurança da informação como:

- Dantas (2011), que em seu livro segurança da informação fala sobre os alicerces que definem o mesmo e os modelos para gerenciamento de riscos e algumas ferramentas.

- Kurose e Ross (2010) descrevem em seu livro, Redes de computadores e a Internet, sobre o gerenciamento de rede de forma bastante didática e nos transmite todo o embasamento técnico, para construção de uma rede gerenciada e os motivos que leva a se ter uma rede gerenciada, em todos os possíveis tipos de redes e as melhores práticas de segurança na Internet.

- Lopes, Sauvé e Nicoletti (2003) propõem em seu livro, Melhores Práticas para Gerência de Redes de Computadores, um guia para ajudar o administrador de redes, de maneira que se crie uma norma a ser seguida e que se padronizem as atividades.

- Stallings (2010), o livro Criptografia e segurança de redes, demonstra a teoria, a prática e os principais indícios para, se desenvolver sistemas que se demonstrem seguros perante a rede de computadores, tais como as informações que nele são armazenadas. Ele também aborda os recursos para a segurança de autenticação via IP e Web.

2 SEGURANÇA DA INFORMAÇÃO

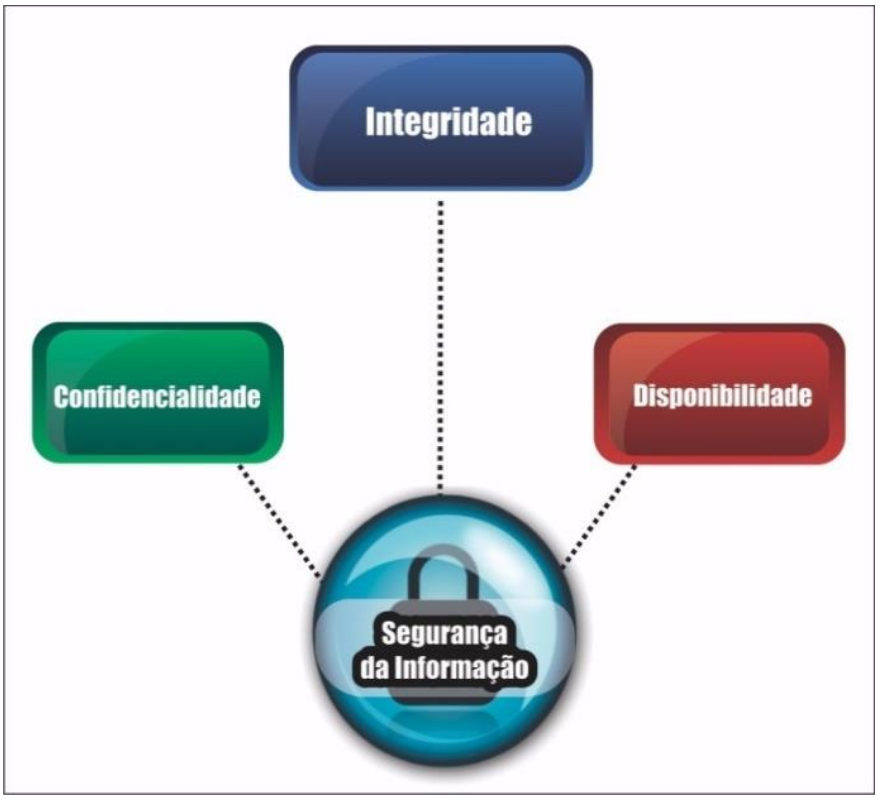
Com o avanço gradativo da tecnologia e informações de dados, é importante garantir os três pilares mundialmente conhecidos como: a integridade, a disponibilidade e a confidencialidade, que são padrões e sempre devem existir para a melhor segurança dos dados.

A segurança da informação tem como objetivo proteger dados, quanto a inúmeros tipos de ameaças para que seja garantida a continuidade do negócio, e diminuir o risco para o mesmo, devendo-se aumentar o retorno do que se tem investido juntamente com as oportunidades de negócio (ISO/IEC, 2005).

O tema segurança da informação tem como objetivo despertar interesse em vários cargos dentro de uma organização, desde executivos, gerentes e até técnicos na área de tecnologia. Isto ocorre porque a segurança cobre diversas áreas de uma organização tais como: segurança física, infraestrutura tecnológica, aplicações e conscientização organizacional. Cada uma delas com seus próprios riscos, ameaças potenciais, controles aplicáveis e soluções de segurança que podem minimizar o nível de exposição ao qual a organização está exposta, com o objetivo de garantir segurança para o seu principal patrimônio: a informação (MAIA, 2013).

A Figura 1 exibe como é dividido os três pilares da segurança da informação, baseado na maioria dos autores da área.

Figura 1 - Pilares da segurança da informação



Fonte: Autoria Própria

2.1 CONFIDENCIALIDADE

Em segurança da informação “Confidencialidade é garantir que toda a informação seja acessada pelo indivíduo ou organização, a que ou quem os dados foram destinados” (DANTAS, 2011, p.13).

Toda informação tem o seu valor, e para que o mesmo seja autêntico os seus dados devem estar íntegros. Para manter a sua integridade, a segurança da informação tem como objetivo proteger contra qualquer acesso não autorizado.

A definição de confidencialidade é proteger dados transmitidos contra-ataques passivos, sobre o conteúdo de uma transmissão de dados, há vários níveis de proteção que podem ser usados. O serviço mais completo tem como parâmetro proteger informações entre dois usuários por um tempo determinado, ou seja, quando uma conexão de tipo TCP é estabelecida entre dois computadores, essa proteção inviabiliza que seja divulgado qualquer tipo de dado transmitido entre os

dois usuários, em outro aspecto é fazer a proteção do fluxo de tráfego contra qualquer análise, isso vai inibir que o atacante veja vários aspectos como, a origem e o destino, a frequência, o tamanho e outras características do tráfego em sistema de comunicação (STALLINGS, 2010, p.10).

2.2 INTEGRIDADE

Em segurança da informação “Integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento” (DANTAS, 2011, p.11).

Segundo Stallings (2010), ter como garantia a integridade da informação recebida é muito importante, pois de nada vale aquilo que não se tem confiança.

A segurança da informação tem como obrigatoriedade garantir que os dados transmitidos ou recebidos, sejam realmente íntegros, desde o seu ponto de partida até o ponto de chegada.

A integridade de dados voltada a conexão, tem um fluxo de dados chegando e saindo, a garantia que é recebida conforme foi enviada sem qualquer tipo de modificação, mostra que a integridade dos dados está totalmente segura.

Quando há ataques ativos, deve-se tratar à detecção ao invés da prevenção, se uma informação é violada, sendo detectada uma intervenção humana será necessária para recuperar a informação tornando-as integras novamente (STALLINGS, 2010, p.10).

2.3 DISPONIBILIDADE

Em segurança da informação “Disponibilidade, é a garantia de que os usuários autorizados obtenham acesso à informação e aos dispositivos correspondentes, sempre que necessário” (DANTAS, 2011, p.12).

Um sistema deve estar disponível, e se oferecer serviços e aplicações sempre que for requisitado pelo usuário deverá ser atendido sem interrupções.

E de acordo com Stallings (2010), a RFC 2828 define que, disponibilidade como propriedade de um sistema ou recurso, deve estar pronta para ser acessado e utilizado em demanda, por uma entidade autorizada do sistema, de acordo com as especificações de desempenho. Vários ataques podem trazer perdas ou reduzir a disponibilidade, alguns deles demonstram ser favoráveis a contramedidas automatizadas, como autenticação e criptografia enquanto outros necessitam da ação física para impedir ou se recuperar da perda de disponibilidade dos elementos de um sistema.

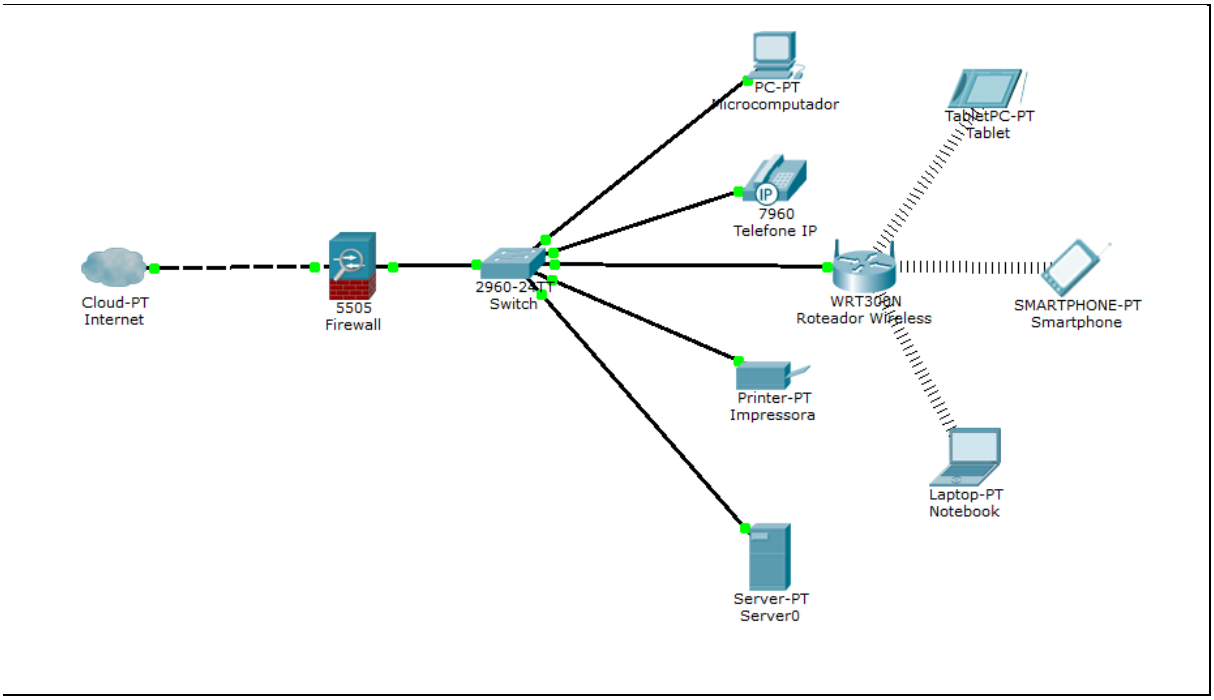
3 GERENCIAMENTO DE REDES

Com a crescente necessidade de se ter um mundo conectado de forma contínua, o grande aumento de periféricos que utilizam a rede de computadores, como os dispositivos: *firewalls*, *switches*, roteadores *Wi-Fi*, *notebooks*, *smartphones*, *tablets*, vídeo games e os eletrodomésticos a forma de se ter uma rede organizada depende de uma aplicação que faça a gerência da rede. Esta evolução ocorreu, para que eles sejam eficientes e facilite a vida tanto de uma organização quanto a vida humana.

Quando um dispositivo fica indisponível na rede, pode-se causar variados prejuízos a uma organização, atrapalhando seus negócios. Visando esta necessidade, a importância com a disponibilidade da informação, tem-se priorizado que, estes dispositivos estejam disponíveis sempre que possível, e caso haja alguma falha, o administrador da rede será avisado rapidamente.

A Figura 2 exibe um exemplo de uma arquitetura de rede corporativa.

Figura 2 - Arquitetura de rede corporativa



Fonte: Autoria própria

O principal objetivo de ter uma rede gerenciada é monitorar e controlar todos dispositivos que nela estejam conectados, seja ele físico, como um servidor ou lógico como uma aplicação, devendo assegurar o nível de qualidade de serviço. Para que esta tarefa seja realizada com sucesso, os administradores de rede devem ter todo o auxílio de um sistema, capaz de monitorar e relatar as possíveis causas de erros.

Este sistema tem como função oferecer uma interface única, com as informações sobre a rede e deve ajudar o administrador com um grande conjunto de comandos, que são utilizados para executar tarefas relacionadas a gerencia de redes (LOPES; SAUVÉ; NICOLLETTI, 2003, p. 17).

3.1 PROPÓSITO DE REDE GERENCIADA

Kurose e Ross (2010) compreendem que quando centenas ou milhares de dispositivos são colocados em conjuntos por alguma organização, para se projetar uma rede, não há surpresa se algum destes dispositivos apresentarem erros ou defeitos, possivelmente porque foram mal configurados, ou que periféricos tenham um uso excessivo ou até mesmo que componentes possam apenas quebrar.

O administrador desta rede deve estar ciente, para que sua intervenção seja imediata. E para que isso ocorra com sucesso é necessário ter ferramentas que ajudem a monitorar, administrar e controlar a rede. Alguns recursos de monitoramento que os autores descrevem em seu livro são:

- Monitoramento de Hospedeiro: Este tipo de monitoramento ajuda o administrador de rede a checar, se todos os hospedeiros da rede estão em bom funcionamento. Com esta ação o usuário pode ter uma boa impressão sobre o administrador, que foi proativo referente à falha antes que o próprio usuário possa ter reclamado.

- Monitoramento de tráfego: Com este recurso o administrador pode se beneficiar encontrando o que está causando um tráfego excessivo em sua rede, e aplicar as melhores práticas para que esse tráfego tenha uma boa fluidez

melhorando toda a LAN (*Local Area Network)* de sua organização, assim deixando os colaboradores contentes.

- Monitoramento de Roteadores: Ao monitorar as tabelas de roteamento, o administrador pode detectar a alternância entre rotas ou mudanças frequentes das rotas, que podem causar instabilidade no roteamento. Com este tipo de alerta o administrador pode reagir antes mesmo que a *internet* fique indisponível.

- Detecção de intrusos: Todo administrador deve estar precavido contra as intrusões de rede, e se puder ser avisado melhor ainda. Este mecanismo pode filtrar os pacotes SYN (*Synchronize*), que é um ataque de negação de serviço de um dispositivo desconhecido, enviado a um servidor de sua rede local. Este tipo de ocorrência pode se concretizar como um ataque à segurança, podendo parar um serviço ou até mesmo o próprio servidor.

- Detecção de mau funcionamento de Hardware: Este mecanismo visa monitorar qualquer falha ou problema de *hardware* de qualquer equipamento de sua LAN, seja ele um *switch*, servidor, roteador e etc.

3.2 MODELO DE GERENCIAMENTO DE REDE

Em seu livro, Kurose e Ross (2010) citam o modelo que a *International Organization for Standard* (ISO) criou para se ter uma rede útil e este modelo é:

- Gerenciamento de desempenho: Ter como meta analisar a medição, quantificação, e controlar todo o desempenho dos dispositivos que estão em sua rede, como exemplo: Um *link* de *internet* com velocidade de 10Mbps está trafegando apenas com 5Mbps.

- Gerenciamento de falhas: Os principais objetivos deste gerenciamento é registrar, detectar e ter uma reação a cada condição de falha da rede, tendo como solução tratar as falhas transitórias da rede como, por exemplo, a interrupção de serviços e aplicações.

- Gerenciamento de configuração: Esta opção permite ao administrador, conhecer os dispositivos que realmente fazem parte de sua rede, e quais são as suas configurações, tanto de *hardware* quanto de *software*. Como exemplo, podem-se definir quais servidores estão com apenas 16GB de memória RAM ou com discos menores que 500GB.

- Gerenciamento de contabilização: Com esta condição o administrador da rede consegue especificar, registrar e controlar os acessos dos usuários e dispositivos de sua rede, e também ter uma definição de quantas páginas uma impressora imprimiu no mês ou a quantidade de trafego que o servidor de FTP *(File Transfer Protocol)* teve em um mês.

- Gerenciamento de segurança: Tem como principal função ajudar o administrador a controlar os acessos aos recursos de sua rede local, visando a política que foi acordada pela organização com os seus colaboradores, como exemplo, saber qual usuário acessou arquivos e pastas restritas sem a devida permissão (KUROSE; ROSS, 2010, pp. 555-556).

3.3 ARQUITETURA DE GERENCIAMENTO DE REDES

Os quatro modelos utilizado para o gerenciamento TCP/IP *(Transmission Control Protocol/Internet Protocol)* é formado pelos elementos a seguir:

- Estação de gerenciamento: A estação de gerência possui o software que se comunica diretamente com os agentes instalados nos dispositivos de rede que vão ser gerenciados, com o objetivo de monitora-los e controla-los. A estação de gerência tem como função ser a interface para os usuários autorizados que estão aptos a gerenciar a rede (LOPES; SAUVÉ; NICOLLETTI, 2003, p. 17).

- Agente de gerenciamento: O agente tem o objetivo de responder as solicitações das informações e das ações da estação de gerenciamento, e também tem o dever de proporcionar a comunicação assíncrona das informações importantes, que foram solicitadas por esta estação. Este software concede

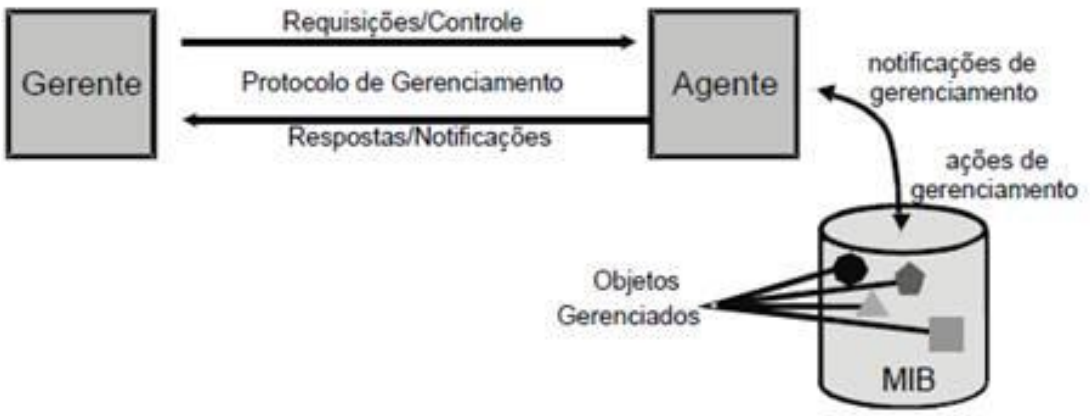
permissão para que o equipamento seja monitorado e controlado através do servidor de gerência (RNP, 1997).

- Base de informações gerenciais (MIB): Caracterizada como um banco de dados ativo, onde possibilita que os valores de suas variáveis sejam recuperados e também alterados, cada dispositivo com o agente instalado, deve ter a sua própria MIB instalada, onde é relacionado com os objetos que estão sendo gerenciados sob o seu domínio (RNP, 1997).

- Protocolo de gerenciamento de redes: A comunicação entre a estação e o seu agente, é definida pelo protocolo da gerência de rede mais conhecido como SNMP *(Simple Network Management Protocol),* que define mensagens, unidades de dados chamadas PDU *(Protocol Data Unit)*, para serem trocadas durante uma comunicação entre o gerente e o agente (RNP, 1997).

A Figura 3 define como é feito as requisições do gerente ao agente instalado no dispositivo que vai ser gerenciado.

Figura 3 - Arquitetura genérica de gerência



Fonte: (TELECO, 2011)

O dispositivo da rede que tiver a capacidade de computação, armazenamento e estar disponível para enviar suas informações relevantes à estação de gerenciamento de rede, são classificados como um dispositivo gerenciável.

Este processo geralmente é realizado pelo *software* presente na estação, que torna possível obter e enviar as informações de gerenciamento, junto aos dispositivos gerenciados. Apenas um processo controla outros inúmeros processos do agente, que podem fazer vários objetos gerenciáveis em um ou mais dispositivos.

Para que este mecanismo funcione corretamente, logo abaixo serão explicados de forma simples e de fácil compreensão, os principais protocolos que são fundamentais para a gerência de redes.

3.3.1 SNMP

Conhecido mundialmente como uma solução de gerência, o SNMP *(Standard Network Management Framework)* que se encontra na versão três (SNMPv3), é um protocolo de gerência que descreve um conjunto de regras que são utilizadas para definir os dados e o conjunto inicial de informações, que já estão prontas para serem usadas.

De acordo com a Teleco (2011), inicialmente recomendado para roteadores, o protocolo SNMP com um nome diferente, chamado de SGMP *(Simple Gateway Monitoring Protocol)* foi desenvolvido continuamente até surgir à primeira versão do SNMP, ele foi lançado no ano de 1991, assim tornando o protocolo como um padrão de fato pelo seu bom desempenho. Foi especificado inicialmente na RFC 1067 em agosto de 1988, e foi evoluindo para as versões SNMPv1 (RFC 1157), SNMPv2 (RFC 1901) até chegar ao SNMPv3 (RFC 2571).

Como um protocolo da camada de aplicação, seu objetivo é facilitar troca de informações de gerenciamento entre os ativos da rede, faz o uso do protocolo UDP *(User Datagram Protocol)* que possui uma PDU *(Protocol Data Unit)*, mais simples se compararmos ao TCP *(Transmission Control Protocol).*

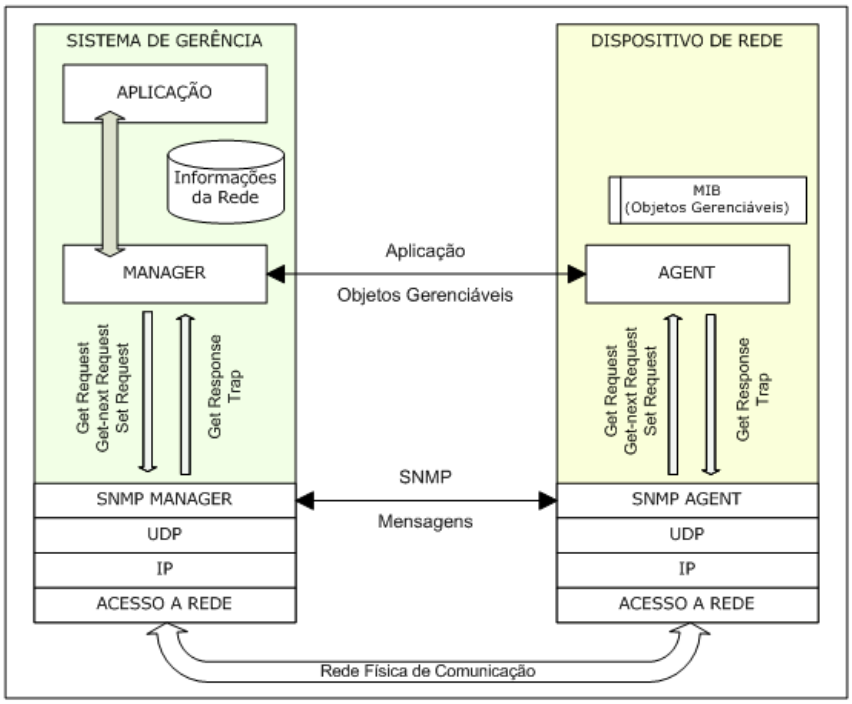
Sua base tem o modelo de gerência da camada OSI e procura informações dentro de um, ou conjunto de domínios, visando gerenciar cada elemento da rede, tornando estatísticas mais relevantes para o bom funcionamento como, utilização, taxa de erros, vazão, nível de colisão e etc (TELECO, 2011).

Por definição quatro componentes básicos tornam o SNMP um protocolo importante para o gerenciamento de redes, e eles são: os nós gerenciados ou agentes, as estações de gerenciamento (gerentes), as informações de gerenciamento (base de dados) e o próprio protocolo SNMP.

“O SNMP é um protocolo relativamente simples e robusto, porém suficientemente poderoso para resolver os difíceis problemas apresentados quando se deseja gerenciar redes heterogêneas” (TELECO, 2011).

A Figura 4 exibe a troca de informações via SNMP, entre o sistema de gerência e o dispositivo de rede.

Figura 4 - Modelo de sistema de gerência SNMP



Fonte: (TELECO, 2011)

3.3.2 SMI

O SMI *(Structure of Management Information)* é um componente do gerenciamento de rede, que tem como papel definir as informações que estão residentes em uma entidade gerenciada da rede.

Isso é necessário para garantir que a sintaxe em conjunto com a semântica dos dados da gerência de rede, seja claramente definida para não apresentar uma indecisão (KUROSE; ROSS, 2010, p. 561).

Praticamente quando o protocolo SNMP é ativado em um sistema, o SMI será ativado em conjunto ajudando a localizar dados que poderão ser gerenciados, como exemplo, os periféricos de um microcomputador sendo eles, memória RAM, processador, disco rígido, tráfego de rede e também os seus processos.

3.3.3 MIB

A MIB *(Management Information Base)* funciona como um banco de dados onde todos os dados coletados dos dispositivos de rede com valores, mostrem o seu estado atual, podendo ser consultado por envio de mensagens. O protocolo SNMP está ligado diretamente ao dispositivo gerenciado (KUROSE; ROSS, 2010, p. 564).

A utilização do MIB necessita avaliar o estado da conectividade de inúmeros objetos da rede, para que o efeito atue no sentido de fornecer a informação relevante, para agente ser criado no dispositivo a ser gerenciado.

Em seguida este agente entra em execução e começa a realizar um teste de conexão, analisando e armazenando o tempo de resposta (LOPES; OLIVEIRA, 2000, pp. 6-7).

A definição da MIB consiste em ser o local de armazenamento utilizado, pelo agente instalado no computador ou servidor que vai ser monitorado, armazenando todo o tipo de dados relevantes, antes ser encaminhada a unidade de gerência.

4 PRTG NETWORK MONITOR

Sucessor do PRTG *Traffic Grapher*, e baseado no sistema operacional Windows, o PRTG Network Monitor foi adequado para redes de pequeno, médio e grande porte, capaz de monitorar LANs, WANs e VPNs, no que se diz respeito à disponibilidade da rede e do uso de banda.

Vários outros parâmetros como qualidade de serviço, carga de memória, uso de CPU, sistemas Linux e Windows, roteadores, *switches*, servidores de e-mail, servidores de arquivos e muito mais, que permite ao gerente da rede ter informações como, relatórios e gráficos de dados que são gerados em tempo real pela própria aplicação (SILVA, 2012, p.2).

O PRTG Network Monitor possui mais de 150 mil administradores de redes atualmente, e consegue monitorar de 10 até 5000 dispositivos redes. Utiliza muitos protocolos para gerenciar redes como o SNMP, WMI, *packet sniffer*, Cisco NetFlow e outros. Tem como principal meta ser um software fácil de instalar e configurar, como interface simples e amigável e com um valor realmente justo, vale lembrar que o software tem uma versão freeware com até 100 sensores disponíveis.

O *software* está disponível apenas para a plataforma Windows, e atualmente conta com nove idiomas como o inglês, alemão, espanhol, francês, português, holandês, tcheco, japonês e chinês simplificado.

Com o seu monitoramento unificado, ele é capaz de monitorar dispositivos de rede, banda de internet, servidores, aplicações, ambientes virtuais, sistemas remotos, IoT *(Internet of Things)* e muito mais.

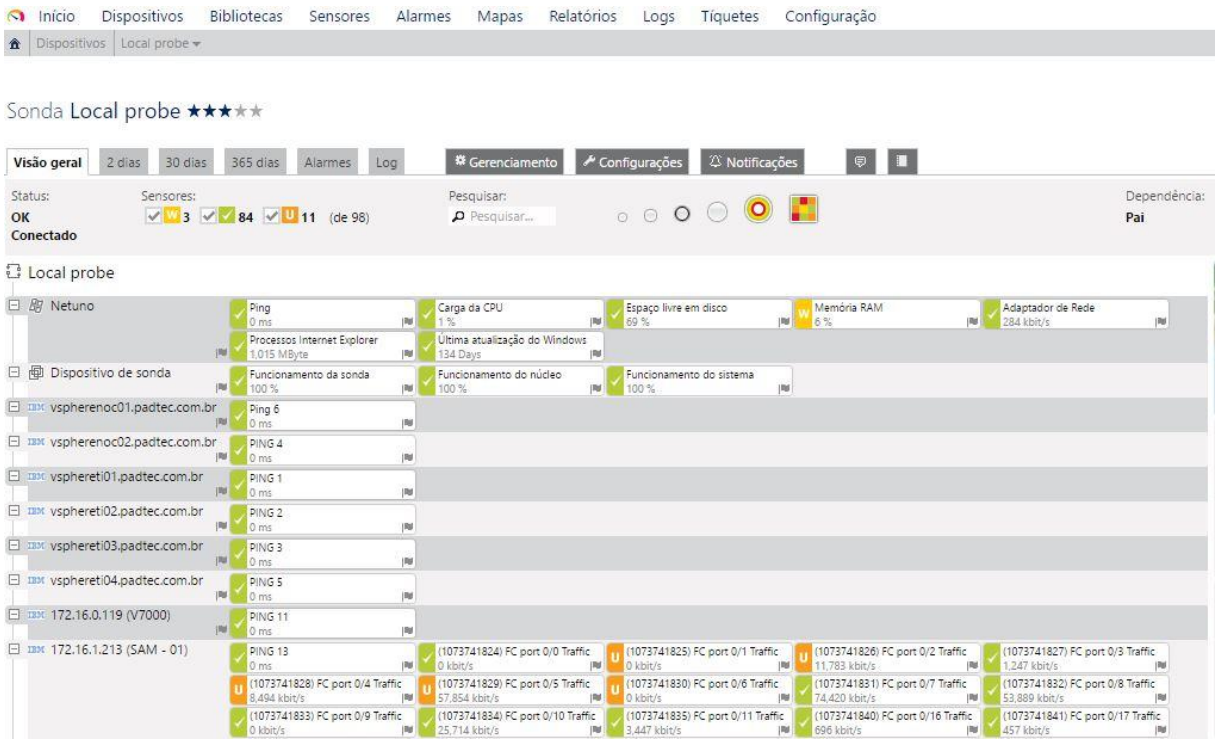
Sua abrangência no mercado conta com as principais aplicações e fornecedores mundialmente conhecidos como Cisco, CITRIX, Microsoft Windows, Oracle, HP, Dell, IBM, VMware, Linux, SQL Server, Microsoft Hyper-V, Amazon AWS e muitos outros, esta abrangência faz com que esta aplicação seja muito mais eficaz, no que se diz respeito a monitoramento e gerência de redes.

Essas redes são a espinha dorsal de uma organização, o tráfego lento de dados ou uma simples queda de energia, podem de alguma forma afetar o negócio da empresa.

Utilizando o PRTG como uma ferramenta de monitoramento contínuo, será muito mais fácil encontrar falhas e repara-las, antes que algum dano seja causado.

A Figura 5 exibe o painel de monitoramento do PRTG Network Monitor:

Figura 5 - Painel de monitoramento



Fonte: Autoria própria

4.1 REQUISITOS DE HARDWARE E SOFTWARE

Toda a estrutura de *hardware* e *software* que será demandada para a instalação do Core Server (Núcleo da ferramenta) assim como da Probe, vai depender dos tipos de sensores e intervalos das varreduras, que serão padronizados pelo administrador (SILVA, 2012, p.3).

Os detalhes informados na Figura 6 são fornecidos pelo próprio desenvolvedor a Paessler.

Figura 6 - Configuração recomendada

Sensores por Servidor de Núcleo	Contas de Usuário	Sondas Remotas	Recomendação de Hardware do Servidor do Núcleo	Espaço em disco (1 ano de retenção de dados)	Virtualização	PRTG Cluster
< 1.000 sensores (ca. 100 dispositivos)	< 30	< 30	2 Cores, 3 GB RAM	250 GB	✓	✓
< 2.500 sensores (ca. 250 dispositivos)	< 30	< 30	3 Cores, 5 GB RAM	500 GB	✓	✓
< 5.000 sensores (ca. 500 dispositivos)	< 20	< 30	5 Cores, 8 GB RAM	1 TB	!	!
< 10.000 sensores (ca. 1,000 dispositivos)	< 10	< 30	8 Cores, 16 GB RAM	2 TB	!	!
Mais de 10.000 sensores	! Por favor, configure servidores PRTG adicionais e contate a nossa equipe de pré-venda.					

✓ = OK
! = não recomendado
! = não suportado

Fonte: Paessler ([s.d])

É recomendado que o PRTG e as sondas remotas as serem instalados em um sistema operacional de arquitetura de 64-bit, em um microcomputador ou servidor, com um hardware que não tenha mais do que dois anos, e de preferência em um Windows Server 2012 R2, com o NET Framework 4.0 ou 4.5 instalados.

A aplicação também é homologada para outras versões do Windows, desde que eles correspondam à arquitetura 64-bit:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

Os outros sistemas operacionais como o Windows Vista e Windows Server 2008, não são recomendados, mas a aplicação pode funcionar corretamente.

4.2 CONSIDERAÇÕES DE DESEMPENHO

De acordo com Paessler ([s.d]), dificilmente alguma instalação terá algum tipo de problema de desempenho, mas por precaução, algumas boas práticas devem ser seguidas para que tudo saia conforme o planejado:

Regra 1, pode se dizer que jamais houve algum tipo de problema de desempenho quando os sensores ficam abaixo de 2.500, com pelo menos trinta sondas remotas e menos de 30 contas de usuários. Se a sua organização possui o cenário descrito pode prosseguir com a instalação normalmente.

Regra 2, se possível sempre use uma máquina física para ter um melhor desempenho, principalmente para organizações com milhares de sensores, pois cada solicitação do sensor terá que passar por muitas camadas de virtualização, que vai custar alto desempenho e medições menos precisas.

Caso seja necessário executar o PRTG em um ambiente virtual é altamente recomendável que fique abaixo dos 2.500 sensores.

Regra 3, para ambiente com cluster do tipo *failover* (redundância entre dispositivos*)*, a carga de monitoramento dobra a cada nó do cluster.

É recomendada uma única configuração de *failover* para o monitoramento de falhas, pois se consistem em dois servidores do núcleo PRTG, e cada um trabalhando com um nó de cluster.

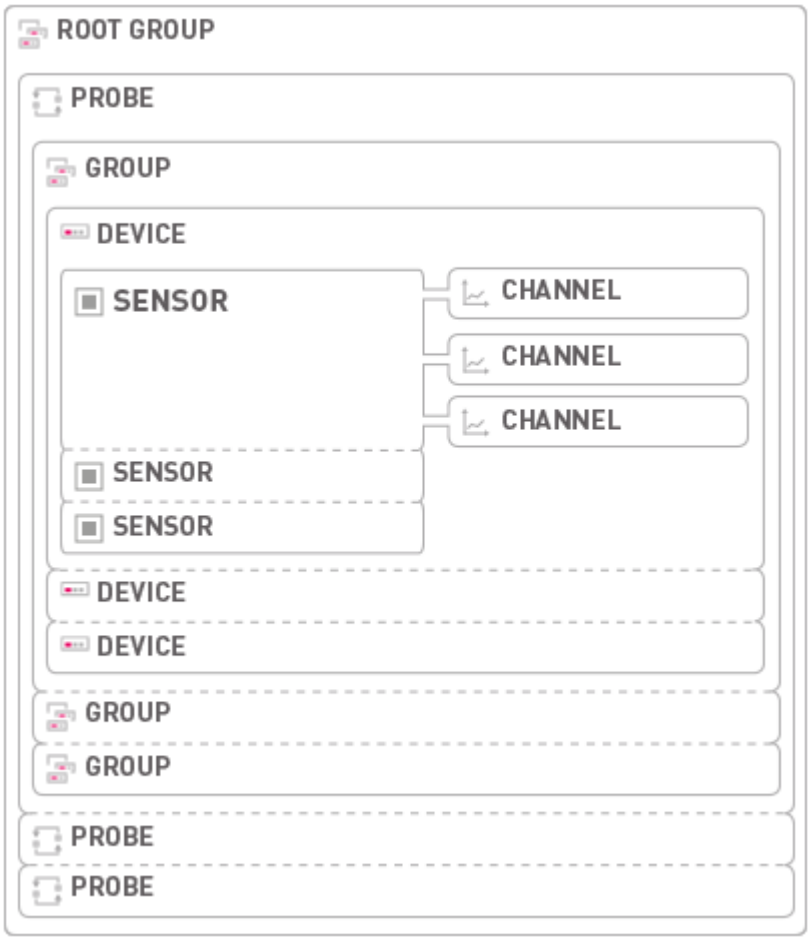
A empresa ainda fornece outras dicas para organizações que usam mais de 2.500 sensores, como usar intervalos de cinco minutos em vez de um ou mais longos. Certos tipos de sensores como de Ping e SNMP, criam menos carga do que sensores mais complexos como o XFlow, VMware, WMI ou sensores de recepção como Syslog/Trap. Ter um limite abaixo de trinta usuários ativos para cada núcleo PRTG, e deixar algumas funcionalidades como mapas, farejadores de pacotes *(packet snnifing),* alocadores de sensor *(sensor factory),* com frequentes detecções para redes extensas e complexas, podem causar certa instabilidade no sistema.

4.3 HIERARQUIA DE OBJETOS

Os objetos são organizados em uma hierarquia do tipo árvore para ter um acesso fácil e dar ao administrador da rede, a opção de organizar em grupos de monitoramento, que são semelhantes com alguns tipos de serviços. A ordem hierárquica relatada, geralmente é usada para definir configurações semelhantes para os grupos de maiores objetos (PAESSLER, ([s.d.])).

A Figura 7 representa a hierarquia do tipo árvore, de uma forma bem organizada.

Figura 7 - Hierarquia de objetos



Fonte: Paessler[1]

[1] Disponível em: <www.paessler.com/manuals/prtg/object_hierarchy>. Acesso em: 09 abr. 2016

Silva (2012), explica a função de cada objeto que está relacionado na hierarquia de objetos:

- Root Group: Este é o grupo raiz na hierarquia de objetos do PRTG, e nele contém todos os objetos que estão sendo gerenciados. Utilizando o mecanismo de herança, é recomendado fazer um ajuste nas configurações padrão do Root Group, para que os outros objetos possam ser herdados.

- Probe: A Probe está ligada diretamente aos grupos com a exceção do grupo Root e todos os objetos configurados abaixo serão monitorados por ela.

- Group: Tem como principal função organizar de forma lógica os objetos que são semelhantes.

- Device: O PRTG entende que cada *Device* (Dispositivo) é possível ser monitorado, nele você poderá adicionar e organizar os ativos da rede que vão ser monitorados.

- Sensor: Com vários tipos de sensores que podem ser configurados nos dispositivos, cada sensor terá a função de monitorar apenas o que foi designado para ele, como exemplo, consumo da CPU, consumo de memória RAM, tráfego de rede e outros.

- Channel: Cada tipo de sensor tem uma série de canais que recebe variados fluxos de tráfego, por exemplo, o canal de sensor de tempo de inatividade de um dispositivo, o canal de tempo de carregamento de uma página web, e o canal de tempo de resposta de um serviço ou aplicação (SILVA, 2012, pp. 6-7).

4.4 SISTEMA DE NOTIFICAÇÕES

Possuindo dez tipos de notificações que podem ser enviados por e-mail, Push, SMS, syslog, Traps SNMP, solicitação de HTTP, registro continuo de eventos, arquivos de som de alarme e Amazon SNS.

As notificações Push por padrão estão disponíveis em todas as licenças do PRTG, as notificações podem ser vistas na área de notificação e também em dispositivos móveis que utilizam sistemas Android ou iOS.

Os tipos de alertas são variados e cada alarme traz informações relevantes, ajudando o administrador de rede, sempre ficar atento com as ocorrências em seus dispositivos de rede.

Nos tópicos abaixo será explicado à funcionalidade de cada alarme, segundo a Paessler:

- Alertas de estado: Este tem como função mostrar as atividades, quedas e advertências de cada dispositivo.

- Alertas de limite: Pode ser configurado um valor limite tanto para cima quanto abaixo de x, como exemplo, se o valor de utilização de CPU ultrapassar 70%, o alerta será exibido relatando este acontecimento.

- Alertas de limiar: Também pode ser configurado um valor definido pelo administrador da rede com valores acima ou abaixo de y minutos, ou seja, se uma aplicação parar de responder por 5 minutos o alerta será gerado relatando esta ocorrência.

- Alertas de condições múltiplas: Este alerta pode ser configurado com a seguinte finalidade, se x e y estão abaixo do valor estipulado, o administrador será alertado, por exemplo, se a memória RAM ultrapassar 90% de uso e uma aplicação ficar por 10 minutos sem responder, esta condição irá alertar sobre este problema.

- Alertas de escalação: Este tipo de alerta irá gerar notificações extras, a cada x minutos, durante o tempo que um dispositivo ou aplicação ficar indisponível.

- Dependências: As dependências são para evitar os acúmulos de alarmes, ou seja, pode ser configurado quando um sensor depende do outro, para que ele funcione. Como exemplo ao monitorar um link dedicado, o sensor de Ping depende que o sensor de DNS esteja ativo e respondendo para que ele funcione corretamente.

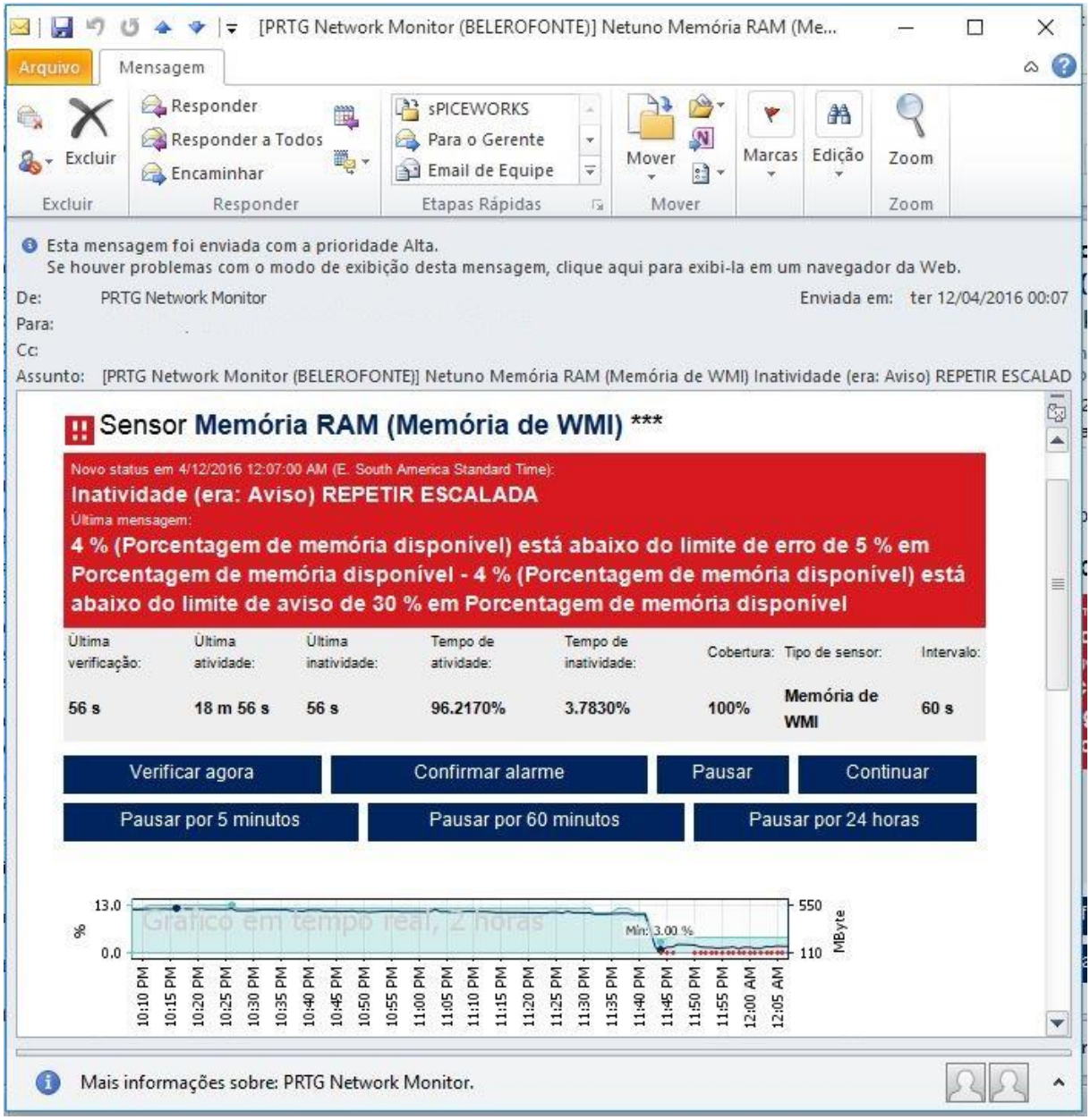
- Alarmes de reconhecimento: Esta notificação aparece quando um dispositivo ou aplicação voltou a funcionar, cessando as outras notificações de ocorrências.

- Agendamento de alertas: Pode ser configurado este tipo de ação, como um alerta de baixa prioridade, apenas para que seja lembrado, de realizar uma

manutenção ou correção de um dispositivo ou aplicação, em períodos de baixo impacto para a organização.

A Figura 8 exibe um alerta real do PRTG que foi enviado por e-mail relatando que um servidor estava com pouca memória disponível.

Figura 8 - Notificação por e-mail



Fonte: Autoria própria

4.5 LICENCIAMENTO E CONTRATO DE SUPORTE

Segundo a Paessler ([s.d]), o licenciamento do seu produto pode ser feito pela quantidade de sensores ativos em sua rede, sendo uma maneira simples e justa. Por definição cada sensor que monitora uma URL específica, ou o tráfego de uma conexão de rede, uma porta de um *switch*, a carga da CPU em um servidor ou qualquer ativo da sua rede, será utilizada entre 5 a 10 sensores para cada dispositivo, lembrando que estes números de sensores podem ser menores dependendo do que exatamente você quer monitorar.

Como exemplo, ao monitorar um servidor vários sensores serão adicionados, mas você pode escolher os sensores que realmente são crucias como, memória RAM, carga de CPU, volume usado do disco rígido e o Ping (Comando que serve para testar a conectividade entre equipamentos), esses quatro tipos de sensor vão deixar o administrador atento, se houver falha em algum servidor.

Com este método você paga apenas o que deseja monitorar, trazendo um custo benefício maior para a sua organização.

O contrato de suporte pode ser escolhido através de planos para a edição licenciada, durante este prazo você pode baixar novas atualizações e versões do produto com direito ao suporte fornecido pela Paessler desenvolvedor do produto, vale ressaltar que o suporte está disponível apenas na língua inglesa.

Ao adquirir um produto licenciado é incluído doze meses de suporte, mas se preferir um contrato de suporte por um período maior, um desconto entre 5 a 10 por cento será abatido do preço final.

A Tabela 1 exibe os preços em dólar, de cada edição do PRTG:

Tabela 1 - Tabela de preços

Licença PRTG	Quantidade de Sensores	Preço
Edição gratuita	100	Sem custo
Edição de teste	Ilimitado	Gratuito por 30 dias
Edição PRTG 500	500	US$ 1.600
Edição PRTG 1000	1000	US$ 2.700
Edição PRTG 2500	2500	US$ 5.600
Edição PRTG 5000	5000	US$ 9.500
Edição PRTG ilimitado	Ilimitado	US$ 13.500
Edição PRTG corporações publicas	Ilimitado	US$ 40.500

Fonte: Baseado em Paessler ([s.d])

5 ANÁLISE EXPERIMENTAL

Toda a coleta de dados foi realizada a partir de um ambiente corporativo realizado com a permissão da empresa Padtec S/A, que é uma empresa voltada ao mercado de soluções em comunicação óptica.

> A Padtec é uma fornecedora global voltada ao desenvolvimento, fabricação e comercialização de soluções turnkey para sistemas ópticos. Seu amplo portfólio inclui equipamentos para acesso corporativo, DCI, SAN Extension, redes metropolitanas e redes multi-terabit de longa distância terrestres e submarinas (PADTEC S/A, ([s.d]).

O PRTG é uma ferramenta crucial para o monitoramento de servidores físicos, *switches*, *nobreaks*, impressoras, banco de dados, aplicações e ambientes virtualizados, mantendo a administração dos dispositivos de rede sempre em bom funcionamento, visando melhorar o negócio da empresa trazendo satisfação para os clientes e colaboradores.

A estrutura de virtualização que a empresa possui atualmente tem como base o VMware ESXi 5.5.0 em cluster de servidores IBM com 230GB de memória RAM, dois processadores Intel® Xeon® CPU E7-4850 @ 2.00GHz e dois discos rígidos de 300GB cada.

O VMware ESXi atualmente está na versão 6.0, e é um dos melhores softwares de virtualização massiva, com inúmeros recursos que tornam o ambiente virtual totalmente confiável e seguro.

Segundo a VMware os recursos importantes que ESXi traz são:

- Confiabilidade e segurança aprimorada: A estrutura de gerência está incorporada na VMkernel, que reduz a área de cobertura em 150MB. Isso proporciona uma superfície de ataque muito pequena a *malwares* e ameaças através da rede, aumentando a confiabilidade e a segurança.
- Implantação e configuração simplificadas: Com poucas opções de ajustes, instalação e uma configuração simples, torna o ESXi uma ferramenta fácil para manutenção e uma estrutura virtual muito consistente.

- Aplicação e atualização de patches simplificadas: Com um número menor de patches e atualizações de segurança, isso traz uma significativa redução nas janelas de manutenção e janelas de manutenção programadas.

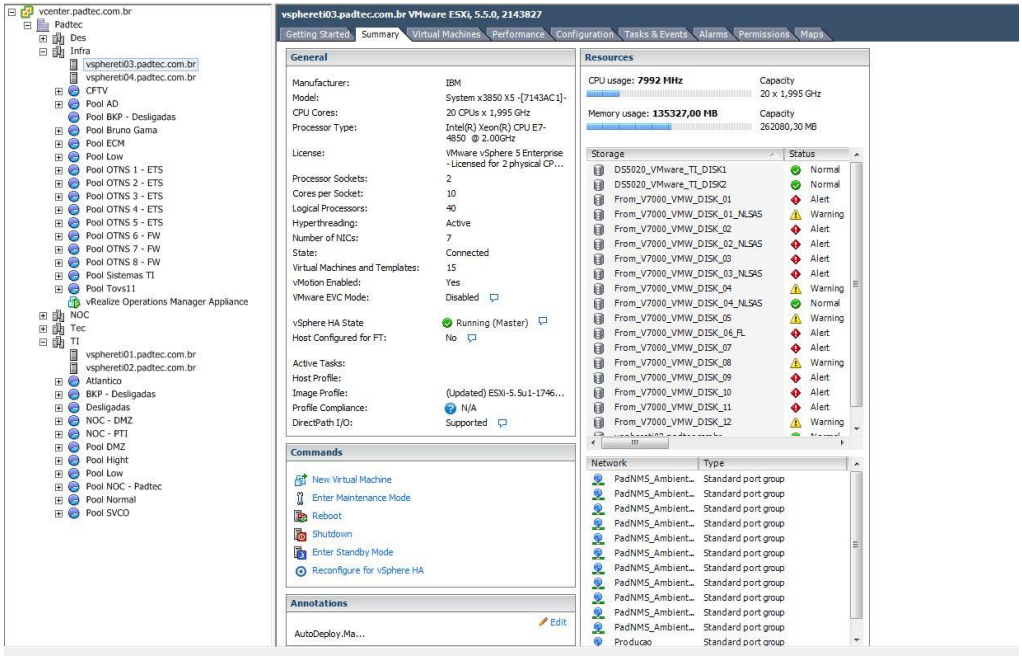
Os detalhes técnicos que o VMware ESXi traz em comparação com os concorrentes é o aprimoramento da segurança, que define os controles de acesso baseado em função, que elimina a dependência de uma conta raiz compartilhada.

Registros em logs e auditoria estendida faz com que o ESXi registre a atividade de todos os usuários tanto no **shell** (Software que oferece comunicação direta, entre o usuário e o sistema operacional) como na interface de usuário, esse registro é feito em **logs,** garantindo a responsabilidade dos usuários, facilitando a auditoria das atividades.

O vMotion, permite realizar a migração de uma máquina virtual inteira de um servidor físico para o outro, sem qualquer tempo de inatividade, mostrando a grande eficiência da aplicação.

A Figura 9 exibe como o VMware ESXi gerencia suas máquinas virtuais, de uma forma simples e intuitiva:

Figura 9 - Gerência VMware ESXi



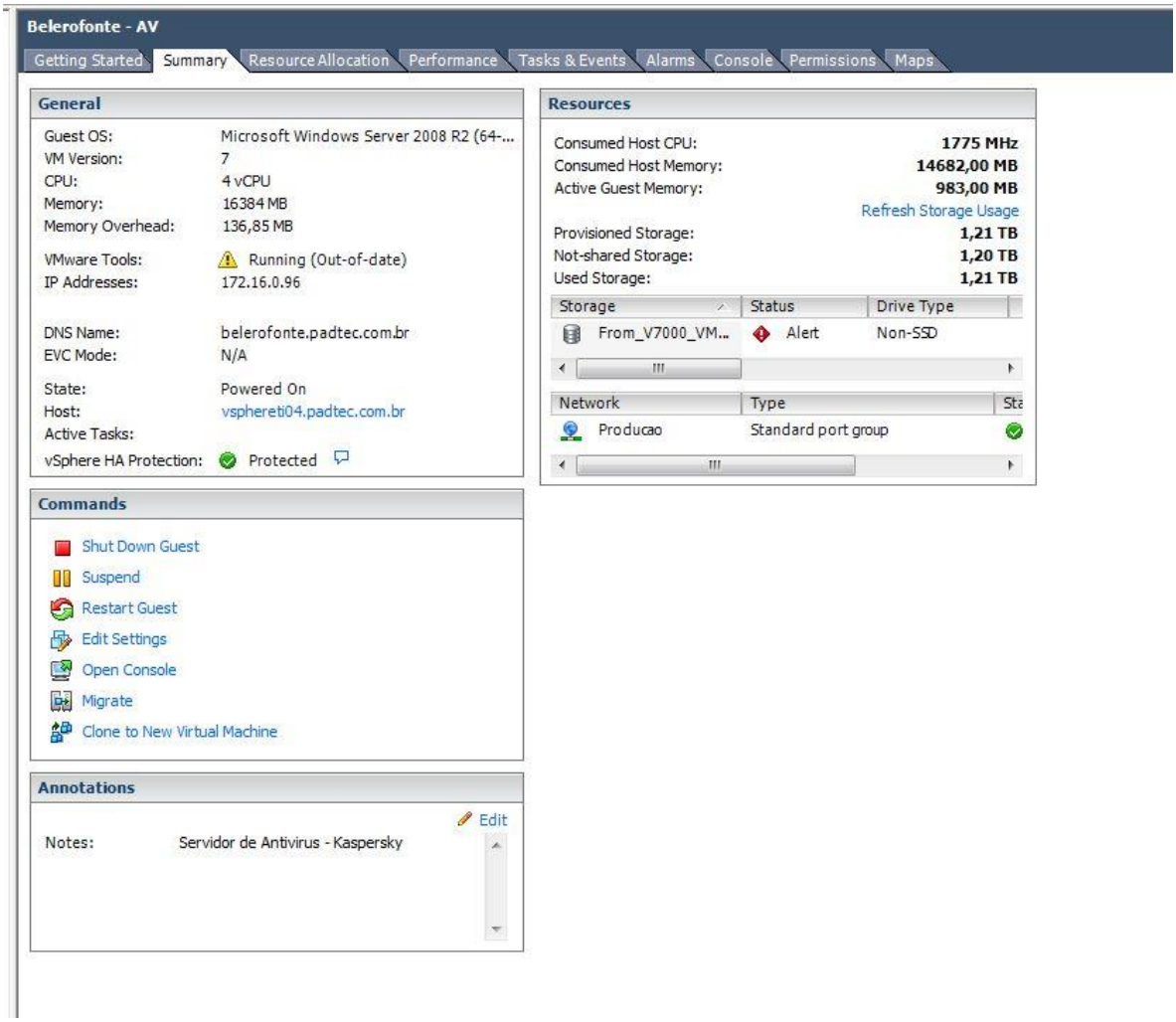
Fonte: Autoria própria

A aplicação do PRTG está instalada em um servidor virtual, com as seguintes configurações:

- Sistema Operacional: Windows Server 2008 R2 Enterprise
- Memória RAM: 16 Gigabytes
- Disco Rígido: 200 Gigabytes
- Processadores: 2 Intel Xeon vCPU E7-4850 2.0 GHz

A Figura 10 exibe detalhadamente as configurações, que foram definidas para a máquina virtual, aonde o PRTG foi instalado:

Figura 10 - Configurações da máquina virtual



Fonte: Autoria própria

Os requisitos acima estão além das configurações, que o desenvolvedor sugere como adequada para o uso do PRTG Network Monitor.

A coleta dos dados foi iniciada a partir do início deste projeto, e foram selecionados os dados de maior valor, para mostrar a eficiência da aplicação deixando o ambiente corporativo em boas condições de funcionamento, conseguindo dar agilidade e segurança aos dispositivos da organização.

5.1 MONITORAMENTO DE UTILIZAÇÃO DE CPU

Este tipo de monitoramento tem como função, medir toda a carga que está sendo processada pela CPU (Central Processing Unit) que corresponde ao cérebro do computador, onde é realizada a maior parte dos cálculos.

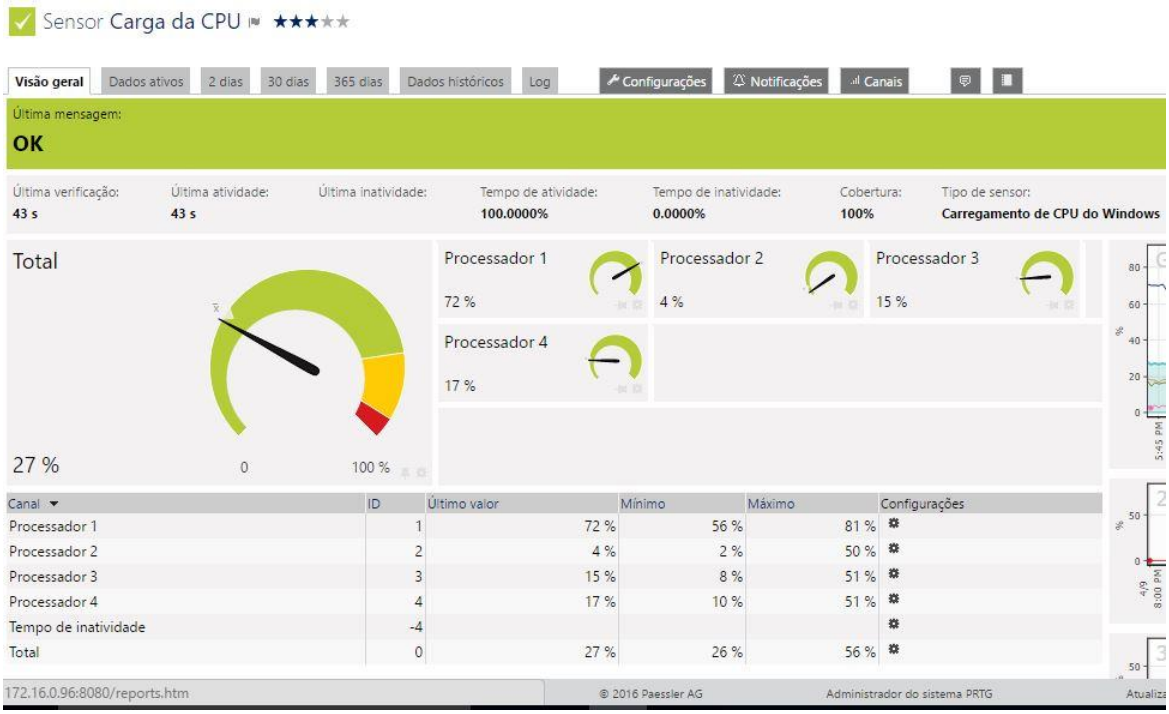
Para este servidor foi configurado o sensor chamado CPU *Usage* (Uso de CPU), os alarmes estão configurados em três etapas, *Warning* (Aviso), *Critical* (Crítico) e *Unusual* (Incomum).

Quando a capacidade de processamento atingir um nível maior que 75% o alarme de *Warning* será disparado, e rapidamente um e-mail será enviado para o administrador da rede dizendo para ter uma atenção a este servidor devido à carga estar como porcentagem alta.

Caso a porcentagem chegue a 90%, o administrador será avisado que a CPU está chegando ao seu limite máximo de processamento, podendo causar interrupções e até travamentos do servidor, afetando as aplicações que nele estão em execução.

A Figura 11 exibe a carga de CPU de um servidor em produção sendo monitorado, exibindo a porcentagem de cada núcleo do processador.

Figura 11 - Carga da CPU



Fonte: Autoria própria

Os limites deste sensor estão configurados para quando a CPU atingir um limite de uso de 80%, o PRTG vai gerar um alerta de aviso que é representada pela cor amarela, e quando atingir 95% de uso será gerado o alerta de critico que é representada pela cor vermelha.

Quando estas condições forem atingidas, o administrador deverá tomar a devida atenção e verificar o que ocorre com este dispositivo, analisando o porquê a CPU está sendo consumida excessivamente.

5.2 MONITORAMENTO DE MEMÓRIA RAM

A função deste monitoramento é analisar o consumo de memória RAM causada pelo sistema operacional e aplicações que nele estão instalados e em execução constantemente.

Os altos níveis de uso da memória podem fazer com que o Servidor seja reiniciado a qualquer momento podendo afetar as aplicações causando certo

prejuízo à organização, vale ressaltar que a memória RAM e a CPU são periféricos cruciais para o processamento de arquivos e aplicações, e qualquer instabilidade que venha ocorrer com esses periféricos, causarão falhas nas aplicações como também no sistema operacional que neste caso é o Windows Server 2008 R2.

A reinicialização forçada do sistema operacional pode corromper a estrutura do mesmo, impossibilitando a sua correção, por isso mesmo que se tenha um sistema de gerenciamento de rede, o backup deve estar em dia.

A Figura 12 exibe a memória RAM deste servidor sendo monitorada, e com os seus limites devidamente configurados.

Figura 12 - Memória RAM

Fonte: Autoria própria

Neste caso real, mais de 88% da memória RAM estava sendo consumida, gerando o alerta de aviso em cor amarela, com a mesnagem que a memória está abaixo do valor definido de 30%, quando este limite chegar em 5% o alerta critico será mostrado no painel e e-mails de alertas serão disparados a cada 5 minutos.

5.3 MONITORAMENTO DE ESPAÇO UTILIZADO EM DISCO RÍGIDO

O monitoramento de disco rígido é essencial, pois ele analisa os espaços em discos tanto físicos quanto unidades lógicas como por exemplo, se um servidor tiver um disco de 1TB de capacidade ele pode ser dividido em unidades lógicas representadas pelas letras do alfabeto, se este disco for dividido em duas partes de 500GB então teríamos a unidade C: com 500GB e a unidade D: com 500GB.

Por padrão do sistema operacional Windows, a letra C sempre representa a unidade de disco onde o sistema operacional está instalado, mas pode ser alterada pela letra que o usuário preferir.

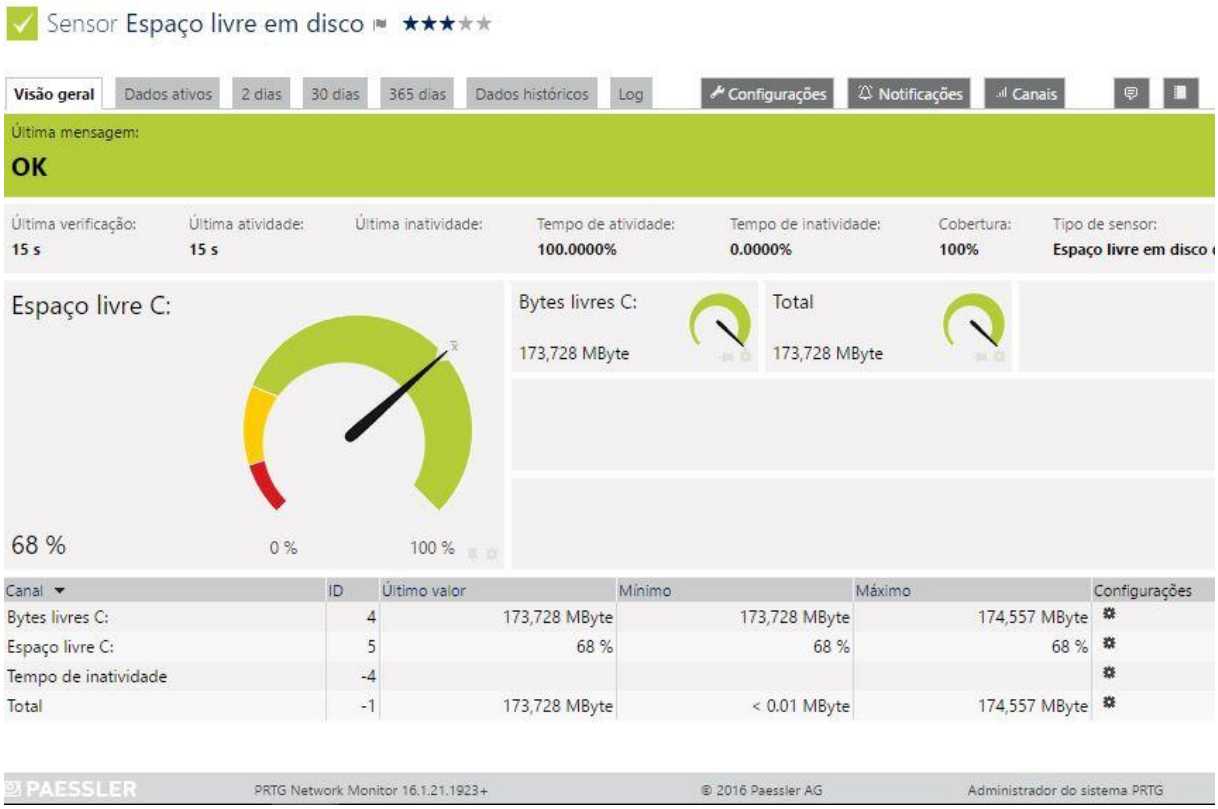
O PRTG tem a capacidade de realizar este monitoramento mesmo que o seu servidor tenha vários discos rígidos e lógicos, mostrando qual é a sua porcentagem de uso, mostrando graficamente a evolução do espaço que foi preenchido ao decorrer dos dias, ajudando o administrador a filtrar por data e ver o que aconteceu por ele ter consumido tanto espaço.

Lembrando que todos os dados e informações que podem ser de extrema importância, inclusive o sistema operacional estão alocados no disco rígido. Por este motivo o monitoramento dele deve estar sempre ativo.

A Figura 13 exibe um disco rigido sendo monitorado em tempo real, e exibe claramente a porcentagem de espaço livre de disco que está representada em MByte, com 68% de sua capacidade que é de 249GB.

Os limites estão configurados em 30% para gerar um alerta de aviso e 10% para gerar um alerta crítico, relatando que o disco está ficando sem espaço de armazenamento.

Figura 13 - Espaço livre em disco



Fonte: Autoria própria

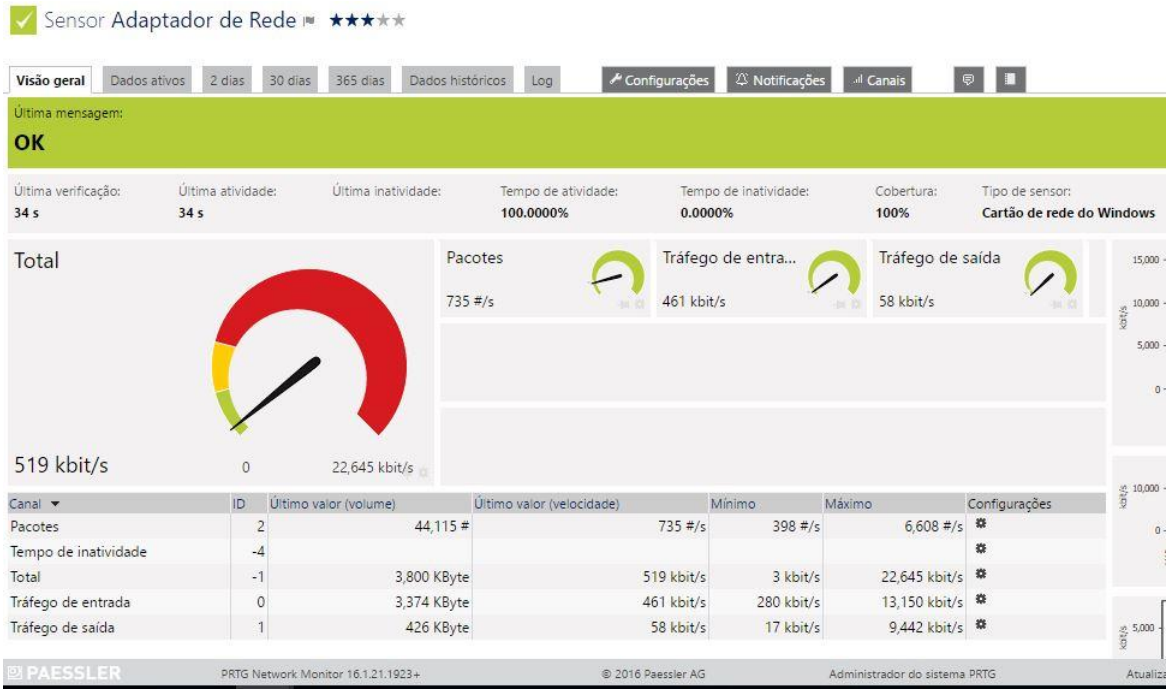
5.4 MONITORAMENTO DE TRÁFEGO DE REDE

Este sensor de monitoramento realiza a filtragem de pacotes, entre o tráfego de entrada e o trafego de saída, ajudando o administrador a entender porquê tantos dados estão entrando e saindo de um determinado servidor.

Este recurso é muito importante, pois a vários tipos de ameaças como vírus, que realizam ataques, e fazem com que o fluxo de dados aumente sem controle até o sevidor ou aplicação ficar indisponivel, este tipo de ataque tem como nome de Ping da morte, isso ocorre quando o atacante dispara inúmeras requisições de Ping para um determinado servidor, até ele não conseguir processar todas as requisições, causando instabilidade e até interrupção dos serviços que estão em execução.

A Figura 14 detalha o monitoramento do adaptador de rede, e o fluxo que nele está ocorrendo.

Figura 14 - Adaptador de rede



Fonte: Autoria própria

Neste caso o tráfego de rede estava em 519KBits/s, o seu limite de aviso estava configurado, para quando o tráfego atingir 10000KBits/s, e o limite crítico configurado para 20000KBit/s.

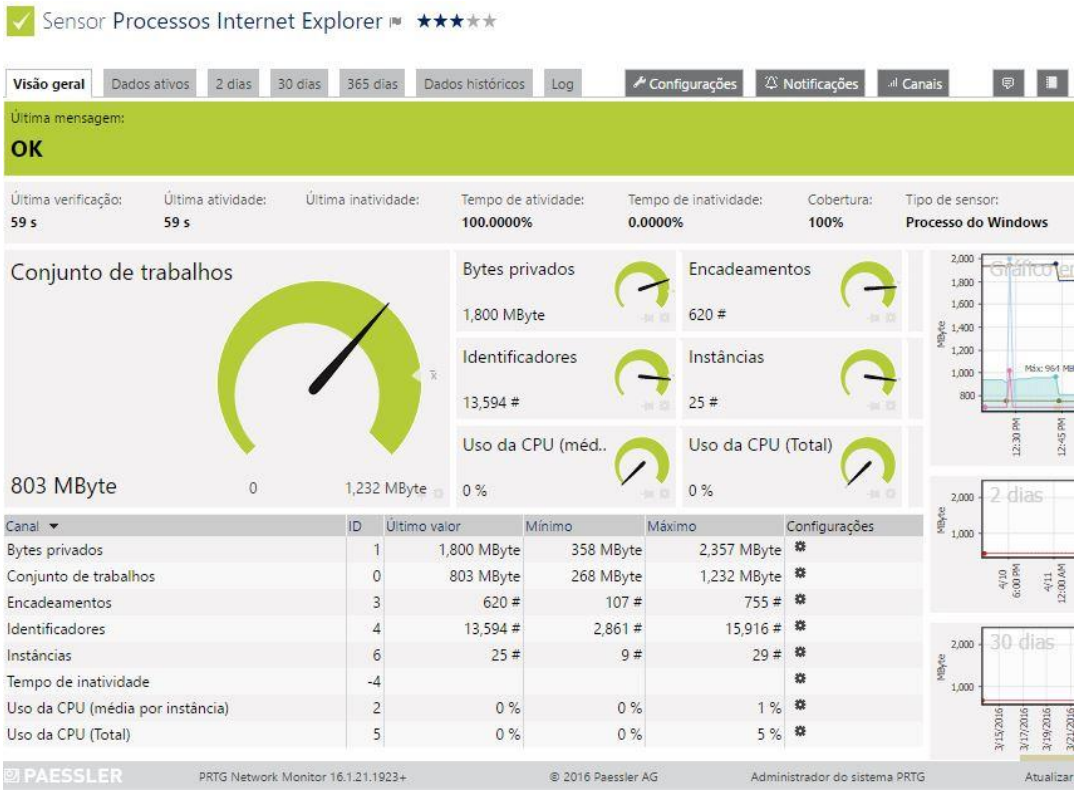
5.5 MONITORAMENTO DE PROCESSO EM EXECUÇÃO NO SISTEMA OPERACIONAL

Com este sensor cada processo que está em execução no sistema operacional, pode ser monitorado sem qualquer dificuldade, lembrando que para muitas empresas existem aplicações que são fundamentais para toda a conjuntura da organização.

Dentro dessas aplicações existem processos e eles ficam em execução até que o mesmo seja fechado. Estes processos têm como a extensão de arquivo chamado de exe (executável), se este processo por ventura trave, seja por falta de memória ou processamento, o monitoramento vai relatar ao administrador este problema, e assim o administrador poderá alocar mais recursos para este processo, evitando problemas como lentidão e instabilidade.

A Figura 15 exibe o monitoramento de uma aplicação chamado Internet Explorer (Navegador de internet), que é utilizado em um servidor, cujo os colaboradores realizam a conexão remota e utilizam o navegador para acessar o sistema ERP *(Enterprise Resource Planning)* software que integra os dados e processo de uma organização em um único sistema, realizando suas tarefas.

Figura 15 - Monitoramento de processo



Fonte: Autoria própria

A imagem exibe o quanto a aplicação está consumindo a memória RAM, que neste caso estava em 803MByte, com o consumo de zero por cento em relação ao processamento.

O monitoramento também detalha quantas instâncias da aplicação estavam em execução, que no momento era de 25.

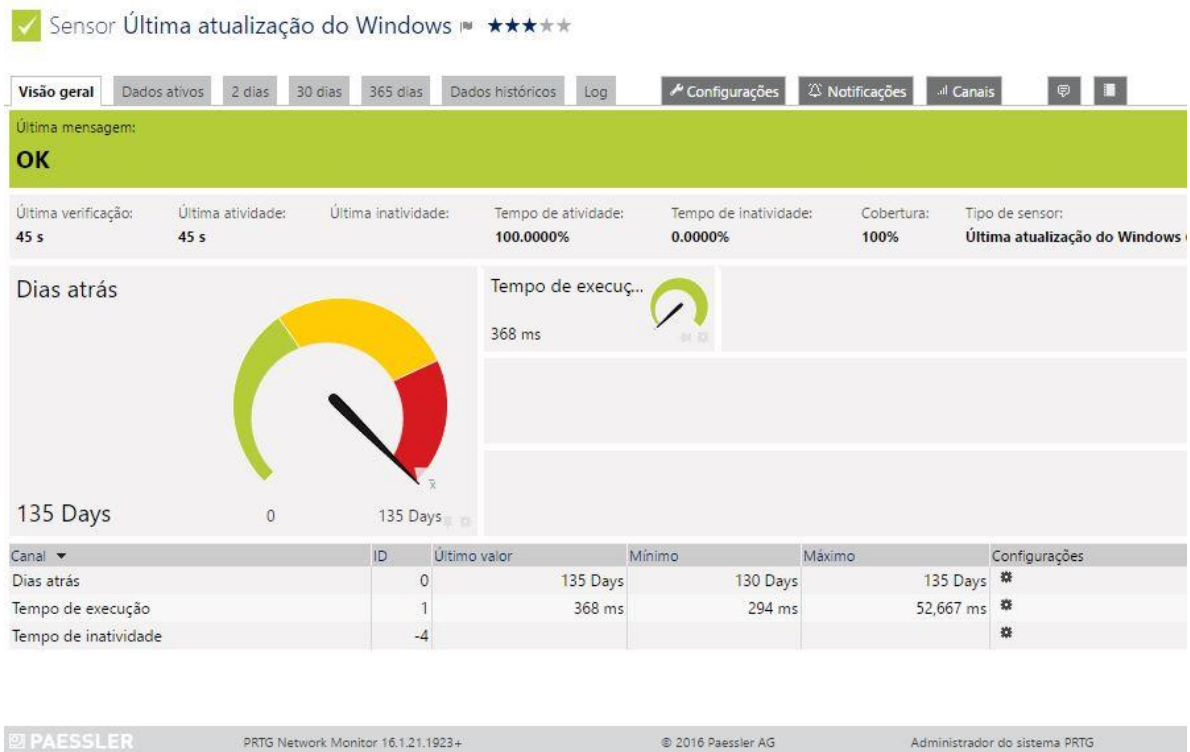
5.6 MONITORAMENTO DE ATUALIZAÇÕES DO SISTEMA OPERACIONAL

Com este tipo de monitoramento o administrador pode acompanhar se o seu servidor ou computador, que utiliza o sistema operacional Windows está em dia com as atualizações de aprimoramento e segurança.

As atualizações são importantes para os sistemas operacionais, pois nelas são corrigidas falhas, que podem causar instabilidade no sistema e vulnerabilidades que podem ser exploradas por *hackers*.

A Figura 16 exibe há quantos dias o sistema operacional estava sem receber atualizações.

Figura 16 - Monitoramento de atualizações



Fonte: Autoria própria

Neste caso o sistema operacional do servidor estava há 135 dias sem atualização, isso é um fato preocupante por se tratar de atualizações que corrigem tantas falhas.

5.7 GRÁFICOS E RELATÓRIOS

O PRTG fornece relatórios e históricos detalhadamente, sobre qualquer dispositivo e seus componentes.

Analisando esses dados, o administrador pode prever as tendências de uso e assim prever quando os recursos se esgotarão como um exemplo típico, o uso de memória RAM tem variações contantes, utilizando o gráfico deste monitoramento pode-se analisar os horários de picos que elevam a utilização desse componente.

A Figura 17 exibe as variações do gráfico, a partir do monitoramento da utilização de memória RAM.

Figura 17 - Gráfico de utilização de memória RAM

Fonte: Autoria própria

Os picos gerados no gráfico, mostram ao administrador os horários que a memória RAM teve maior utilização com variações ao longo do dia**.**

5.8 CONFIGURAÇÕES DE NOTIFICAÇÕES

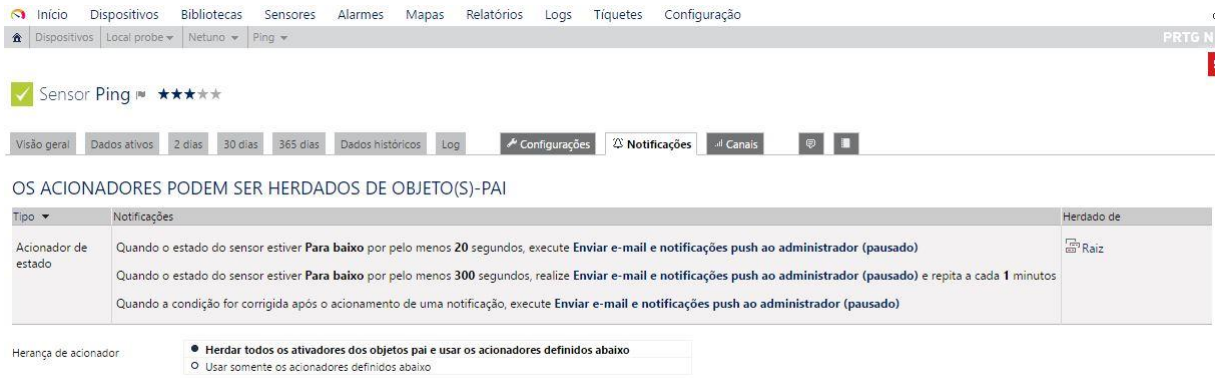
Os estados ou dados de um sensor quando estão em alerta de **Aviso** ou **Critico**, podem disparar notificações via e-mail ou SMS para celular, que ajuda o administrador a ficar sabendo o que está acontecendo em sua rede, mesmo que ele não esteja na organização, os alertas podem ser configurados de acordo com a sua necessidade.

Por exemplo, quando um sensor de Ping passa do estado OK para o estado Critico, o PRTG vai enviar o alerta por e-mail e para o celular que nele foi configurado, informando que certo dispositivo não está respondendo ao sensor de Ping.

Para configurar este tipo de alerta, basta clicar sobre o sensor de Ping do dispositivo selecionado, e em seguida clicar na aba Notificações.

A Figura 18 exibe como são as configurações de notificações de um sensor.

Figura 18 - Configuração de notificações



Fonte: Autoria própria

As configurações de notificações mostram que, quando o sensor estiver **Para Baixo** ou seja não estiver respondendo por pelo menos 20 segundos, o alerta de

aviso será enviado por e-mail, notificações push que são mostradas no painel de monitoramento e via SMS, caso o celular esteja cadastrado.

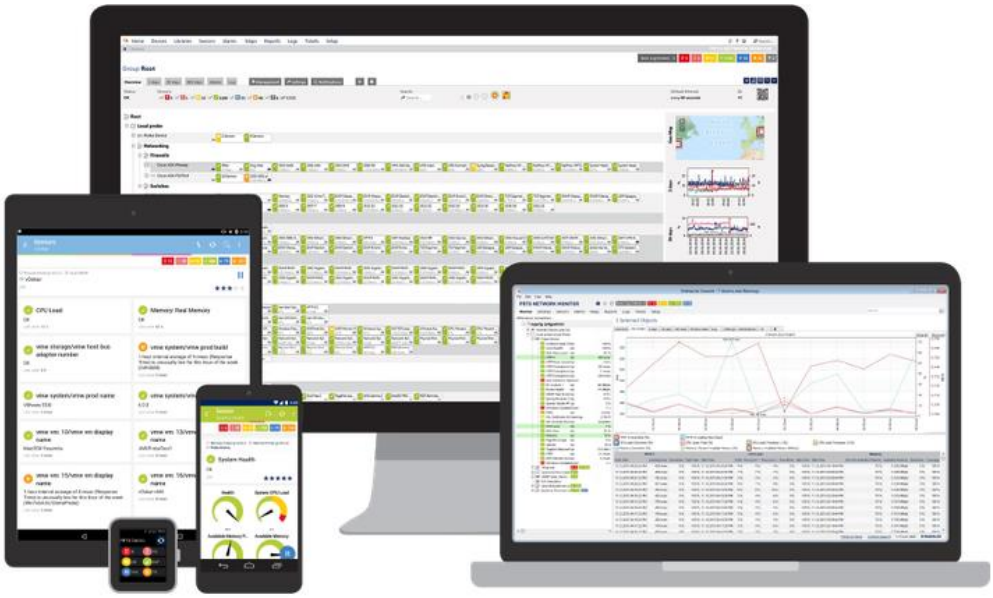
E se este mesmo caso acontecer, e o sensor ficar por mais de 300 segundos sem resposta, será enviado um alerta a cada 1 minuto com a mensagem com estado Critico.

Os alertas que são enviados, chegam de uma forma simples e de fácil entendimento, relatando o horário que este sensor foi parado, com gráficos que mostram como sensor estava reagindo em um determinado periodo, o PRTG tem três tipos de gráficos para cada sensor, com intervalos de uma hora, dois dias e um mês.

As notificações podem ser observadas e recebidas em diefrentes plataformas, o paínel de monitoramento do PRTG pode ser visualizado em um computador, *smartphone*, *smartwatch* e *tablet*, estes aplicativos estão disponiveis para Windows, Android e iOS.

Conforme a Figura 19 exibe, as notificações que são detalhadas e de fácil entendimento, o painel de monitoramento ajuda o administrador a entender o que está acontecendo com cada sensor e dispositivo em sua rede.

Figura 19 - PRTG Multiplataforma



Fonte: Paessler ([s.d])

6 CONSIDERAÇÕES FINAIS

A utilização da ferramenta PRTG Network Monitor, traz muitos benefícios quando tratamos de monitoramento de redes, mas alguns pontos devem ser considerados.

O software se torna uma desvantagem em situações que podem se tornar um problema, caso a organização futuramente tiver um grande aumento de dispositivos e os sensores gratuitos que são apenas 100 não for o suficiente, a empresa terá que arcar com custos para se ter uma licença paga, gerando um custo para a organização que ela pode não estar preparada para realizar o pagamento, sendo assim alguns de seus dispositivos irá ficar sem o monitoramento.

Apesar dessa desvantagem, o PRTG Network Monitor mostrou por suas funções e características, que é uma aplicação que se destaca entre as melhores ferramentas de gerenciamento de redes, conforme mostrado neste projeto.

Toda a estrutura do PRTG assim como os seus sensores, relatórios, gráficos e notificações são de compreensão relativamente simples e muito intuitiva.

Através dos dados e gráficos gerados, o administrador pode identificar diversos dispositivos em sua rede, que estão com cargas excessivas e não estão conseguindo suportar toda a demanda de aplicações e processos que estão em execução.

O PRTG de forma simples e ágil, consegue identificar estes problemas em processadores, memórias, discos rigidos, placas de rede, impressoras, *no*breaks e *switches* e aplicações que estão com falhas ou defeitos, sejam eles problemas fisicos ou lógicos, e a partir desses dados coletados o administrador pode elaborar um plano de ação para ajustar ou realizar a manutenção nestes dispositvos, sem causar impacto na organização.

Os sensores que estão em forma de templates criados pela desenvolvedora, e traz inúmeras inovações para a aplicação e atualizações constantes, que mantém o sistema pronto para monitorar as novas tecnologias.

Sua parceria com as maiores fabricantes e desenvolvedores como IBM, HP, VMware, Cisco, DELL, Cannon, APC e varias outras marcas que são renomadas no mercado de tecnologia, o tornam um grande sistema de monitoramento de redes.

De uma forma geral o PRTG Network Monitor é uma ferramenta que cumpre o seu papel quando se trata de monitoramento de redes, podendo ser instalada e configurada em equipamentos com hardware de pouco poder de processamento.

Com sua licença gratuita que não tem nenhuma limitação, em comparação com as licenças pagas, incluindo todos o sensores disponíveis e atualizações de melhorias que são disponibilizadas para o produto, o tornam uma excelente ferramenta de gerência de redes.

Por este motivo o PRTG Network Monitor foi escolhido para ser apresentado neste projeto mostrando aos administradores de redes o quão util esta ferramenta pode ser no dia a dia.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005; Tecnologia da informação; código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BRASILIA. Rede Nacional de Ensino e Pesquisa. Rede Nacional de Ensino e Pesquisa (Ed.). **Introdução a gerenciamento de redes TCP/IP.** 1997. Disponível em: <https://memoria.rnp.br/newsgen/9708/n3-2.html>. Acesso em: 07 mar. 2016.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** uma abordagem top-down. 5ª Ed. São Paulo: Pearson, 2010.

LOPES, Rui Pedro; OLIVEIRA, José Luís. **Descrição e implementação de uma MIB para sistemas MASIF.** 2000. Disponível em: <https://bibliotecadigital.ipb.pt/handle/10198/4718>. Acesso em: 07 mar. 2016

LOPES, Raquel; SAUVÉ, Jacques; NICOLLETTI, Pedro. **Melhores práticas para a gerência de redes de computadores.** Rio de Janeiro: Campus, 2003. 371 p.

MAIA, Marco Aurélio. **O que é segurança da informação.** 2013. Disponível em: <http://segurancadainformacao.modulo.com.br/seguranca-da-informacao>. Acesso em: 14 mar. 16.

NIC.BR (NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR). Introdução ao gerenciamento de redes; Parte 4; SNMP. Publicado em 13 de abril de 2014. Disponível em: < https://www.youtube.com/watch?v=PqgDoG4gLK0>. Acesso em: 09 abr. 2016.

PAESSLER AG (Alemanha). **PRTG: finalmente um software de monitoramento de rede poderoso e fácil de usar.** Disponível em: <https://www.br.paessler.com/prtg>. Acesso em: 09 mar. 2016

PAESSLER AG (Alemanha). **Requisitos do sistema para PRTG Network Monitor.** Disponível em: <https://www.br.paessler.com/prtg/requirements>. Acesso em: 13 mar. 16.

PAESSLER AG (Alemanha) (Ed.). **Características do PRTG Network Monitor.** Disponível em: <https://www.br.paessler.com/prtg/features>. Acesso em: 20 mar. 16.

PAESSLER AG (Alemanha). **PRTG Network Monitor Licenses and Prices.** Disponível em: <https://www.paessler.com/prtg/price_list>. Acesso em: 21 mar. 2016.

PAESSLER AG (Alemanha). **PRTG Manual: object hierarchy.** Disponível em: <www.paessler.com/manuals/prtg/object_hierarchy>. Acesso em: 09 abr. 2016.

PADTEC S/A (Campinas). **Padtec.** Disponível em: <http://www.padtec.com.br>. Acesso em: 14 maio 2016.

PADTEC S/A (Campinas). **Sobre a Padtec:** Quem Somos. Disponível em: <http://www.padtec.com.br/sobre-a-padtec/quem-somos/>. Acesso em: 14 maio 2016.

RFC 1157. A Simple Network Management Protocol (SNMP). USA: IETF, 1990. Disponível em: <https://www.ietf.org/rfc/rfc1157.txt>. Acesso em: 16 fev. 2016.

RFC 1155. Structure and Identification of Management Information for TCP/IP - based Internets. USA: IETF, 1990. Disponível em: <https://www.ietf.org/rfc/rfc1155.txt>. Acesso em: 16 fev. 2015.

RFC 3418. Management Information Base (MIB) for the Simple Network Management Protocol (SNMP). USA: IETF, 2002. Disponível em: <https://www.ietf.org/rfc/rfc3418.txt>. Acesso em: 16 fev. 2015.

SILVA, Rafael Brianezi da. **PRTG Network Monitor - Solução para monitoração de redes e serviços.** 2012. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS11/Rafael Brianezi da Silva _ Rafael Brianezi da Silva _ Artigo.pdf>. Acesso em: 05 mar. 2016.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. 4. ed. Campinas: Pearson, 2010. 494 p.

STALLINGS, William. **Criptografia e segurança de redes.** 4. ed. São Paulo: Pearson, 2010. 494 p.

TELECO (Ed.). **Gerenciamento e monitoramento de rede I: teoria de gerência de redes.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes1/pagina_2.asp>. Acesso em: 20 mar. 2016.

TELECO (Ed.). **Gerenciamento e monitoramento de rede I: teoria de gerência de redes.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes1/pagina_3.asp>. Acesso em: 07 mar. 2016.

VMWARE (Estados Unidos). **VMware ESXi.** Disponível em: <http://www.vmware.com/br/products/esxi-and-esx/overview>. Acesso em: 23 abr. 2016.

APÊNDICE A – INSTRUÇÕES PARA A INSTALAÇÃO DO PRTG NETWORK MONITOR

1 DOWNLOAD

Para realizar o download da ferramenta PRTG Network Monitor, basta acessar o link https://www.br.paessler.com/ e clicar na opção Download Gratuito, esta opção vem com o PRTG totalmente gratuito com até cem sensores disponíveis.

A Figura 20 exibe a página de download no site da Paessler.

Figura 20 – Download do instalador

Fonte: Paessler ([s.d])

Após clicar, o download irá iniciar automaticamente, em arquivo de extensão **(.zip)**, para abrir ou extrair este tipo de arquivo basta utilizar qualquer software de descompactação de arquivo tais como: **Winrar**, **Winzip**, **7-zip** e etc.

2 INSTALAÇÃO

Após descompactar o PRTG, clicar duas vezes com o botão esquerdo do mouse, no arquivo **PRTG Network Monitor 16.2.23.3269 Setup Freeware and Trial (Stable).exe,** aguarde que a instalação irá iniciar.

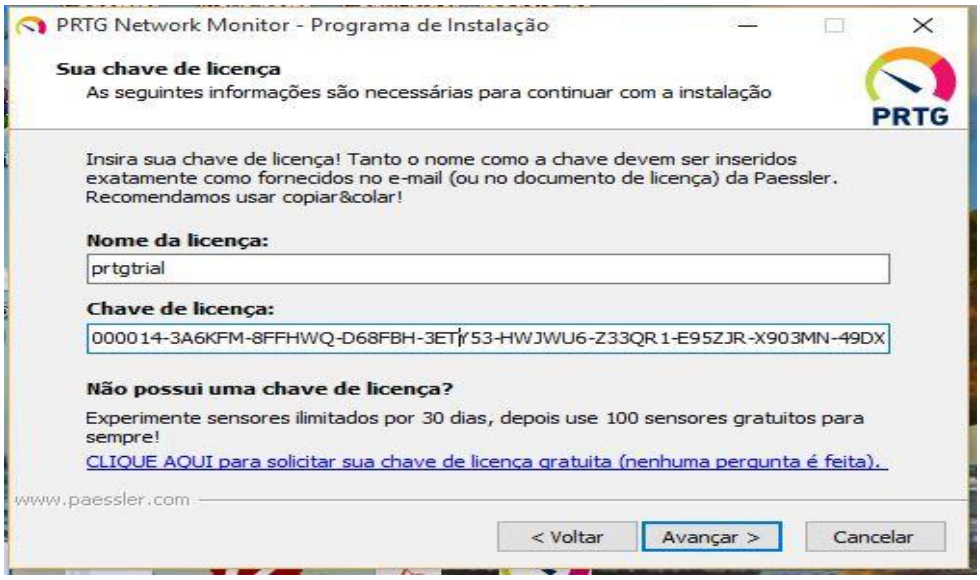
Na primeira parte o aplicativo irá pedir que selecione o idioma a ser utilizado, após selecionar, basta ler e aceitar o termo de contrato de uso e clicar em avançar.

A próxima tela pede para que o usuário digite um endereço de e-mail válido, pois são para este endereço que os alertas gerados pelos dispositivos de rede vão ser enviados.

No próximo passo o usuário deve colocar o nome da licença e sua respectiva chave de ativação, no caso de uma licença gratuita que é o caso deste projeto, o nome da licença e chave de licença é **prtgtrial** e a chave de ativação **000014-3A6KFM-8FFHWQ-D68FBH-3ETY53-HWJWU6-Z33QR1-E95ZJR-X903MN-49DX5G.**

A Figura 21 exibe os campos para inserir o nome da licença e a chave de ativação.

Figura 21 – Ativação do produto

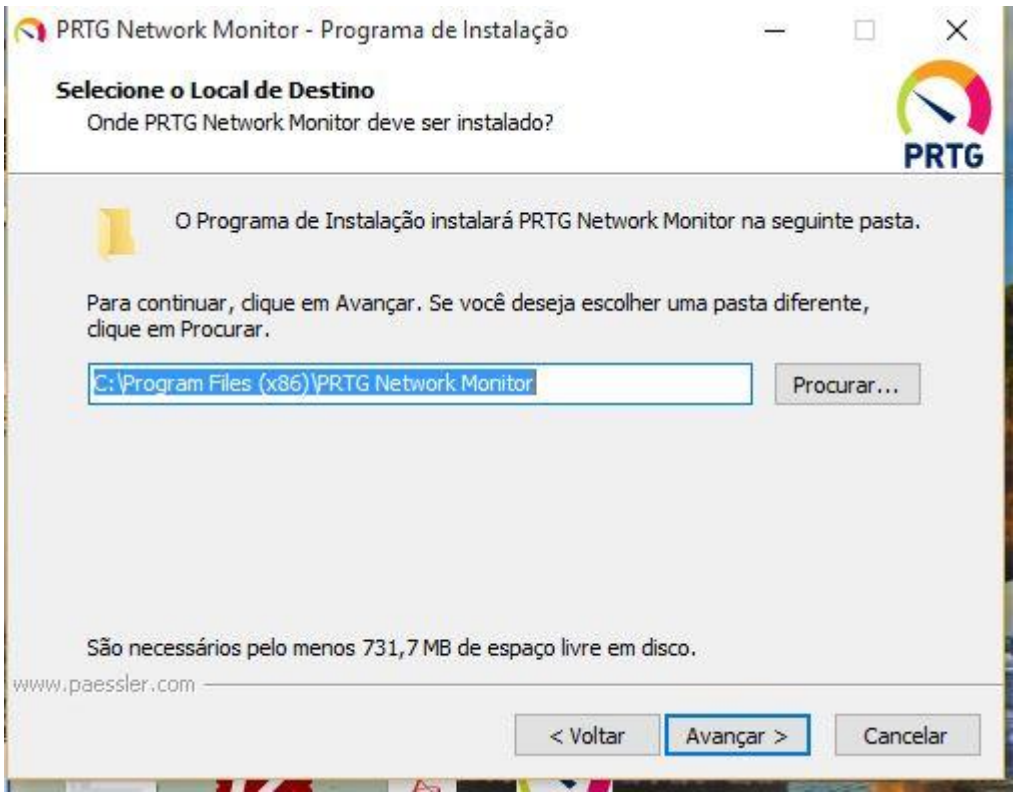


Fonte: Autoria própria

Após a ativação, o PRTG dá a opção de selecionar em qual pasta o usuário quer que a instalação seja feita, por padrão a pasta **C:\Program Files (x86)\PRTG Network Monitor** já vem selecionada, se prefirir mudar o local de instalação basta clicar em **Procurar** e selecionar a pasta desejada, após isso clicar em avançar para que a instalação comece à ser feita.

A Figura 22 exibe como selecionar ou avançar, com o local de instalação.

Figura 22 – Seleção de pasta para instalação



Fonte: Autoria própria

3 CONFIGURAÇÕES BÁSICAS

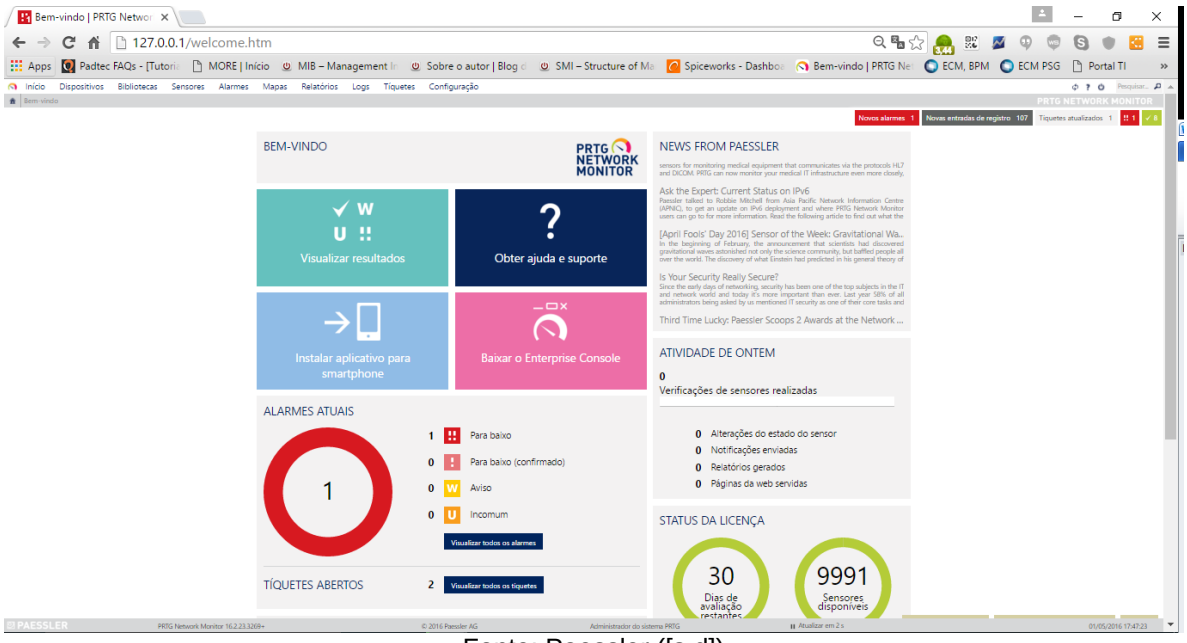
Após a conclusão da instalação, um ícone será adicionado na área de trabalho do computador com o nome de **PRTG Enterprise Console**, clique duas vezes sobre este ícone e logo em seguida será aberta a tela do console do PRTG onde o usuário podera ver todas as conexões de servidores do PRTG.

Para abrir o painel de monitoramento basta entrar no endereço **http://127.0.0.1/** em seu navegador de internet (Google Chrome, Firefox, Internet Explorer e etc), após isso será aberta a tela de bem vindo, aonde o usuário poderá ver os resultados dos dispositivos que foram achados pelo o escaneamento do PRTG, e outras opções que o painel de monitoramento oferece como:

Ajuda e suporte, Visualizar resultados, instalar aplicativo para smartphone e baixar o enterprise console, e também visualizar os alarmes de dispositivos que estão com falhas.

A Figura 23 detalha as opções da tela inicial do PRTG.

Figura 23 – Tela inicial do PRTG



Fonte: Paessler ([s.d])