DESTAQUES ACADÊMICOS
UNIVATES | CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
Revista Destaques Acadêmicos, Lajeado, v. 13, n. 4, 2021. ISSN 2176-3070
DOI: http://dx.doi.org/10.22410/issn.2176-3070.v13i4a2021.3037
http://www.univates.br/revistas

MONITORAMENTO DE REDES DE COMPUTADORES UTILIZANDO O PROTOCOLO SNMP

Ramon Hentges[1], Maria Claudete Schorr[2]

Resumo: O aumento da rede de computadores dos prédios municipais de um município do Vale do Taquari - RS, trouxe a necessidade de monitorar os seus equipamentos, como *switches*, impressoras, dentre outros. Visto este crescimento, monitorar cada equipamento individualmente se tornou uma tarefa que demanda muito tempo. Este trabalho tem como objetivo automatizar o monitoramento dos equipamentos que são compatíveis com o protocolo SNMP na versão 2c. Assim, foi desenvolvido um sistema web de monitoramento de redes através de uma pesquisa acadêmica de caráter experimental e de abordagem quali-quantitativa. A coleta de dados foi realizada de duas formas, uma de forma automática pela ferramenta e outra pelo registro dos chamados de suporte que fizeram uso dela, ambas durante o período de um mês e doze dias. A análise dos dados foi realizada a partir da compilação das informações coletadas, demonstrando os problemas encontrados e pontos em que obteve sucesso. A ferramenta demonstrou ser muito eficaz na detecção de falhas, além de manter o histórico dos problemas e das informações coletadas dos equipamentos. O uso da ferramenta auxiliou o suporte a resolver problemas relatados pelos usuários e demonstrou quais pontos da rede possuem um maior grau de utilização.

Palavras-chave: Monitoramento. Protocolo SNMP. Redes. Gerenciamento.

1 INTRODUÇÃO

No decorrer do crescimento tecnológico mundial, a área de redes de computadores se tornou muito importante para a humanidade, pois com ela temos acesso a informação, comunicação interpessoal, compras, dentre muitos outros serviços benéficos à sociedade, o que tornou a Internet fundamental para todos.

Atualmente temos a Internet como a maior rede de computadores do mundo. Segundo Kemp (2021), ela possui cerca de 4,66 bilhões de usuários,

1 Bacharel em Engenharia de Software, Universidade do Vale do Taquari - UNIVATES.

2 Doutora em Informática na Educação, Universidade Federal do Rio Grande do Sul - UFRGS.

fazendo uso de diversos meios de transmissão, conectando computadores de vários portes, permitindo que seus usuários troquem uma enorme quantidade de informações simultaneamente.

Tendo em vista este enorme crescimento da rede de computadores, o monitoramento individual de cada equipamento que a compõem se torna muito difícil, o que pode levar muito tempo do administrador ao acessar cada dispositivo e verificar seu estado, tempo este que poderia ser melhor gasto em outras tarefas.

Com o avanço da tecnologia, é possível desenvolver ferramentas capazes de monitorar automaticamente cada equipamento desejado, cabendo ao administrador configurar o aplicativo com as especificações desejadas, passando a receber alertas e informações da rede, auxiliando na resolução de problemas e o avisando deles.

Com base nisso, este trabalho apresenta uma forma de auxiliar os administradores de rede no monitoramento de seus equipamentos,0 utilizando o Protocolo Simples de Gerência de Rede (*Simple Network Management Protocol* - SNMP) na versão 2c, disponível em praticamente qualquer dispositivo que se conecte à rede, num sistema web em React e NodeJS, ferramentas de programação JavaScript em ascensão mundial.

2 REFERENCIAL TEÓRICO

Neste capítulo são apresentadas as referências bibliográficas pesquisadas para o embasamento teórico deste artigo, bem como os conceitos gerais sobre o monitoramento de ativos de rede, e o protocolo SNMP.

2.1 Redes de Computadores

Tanenbaum (1996) classifica as redes de computadores como um grande número de computadores independentes, porém interligados, que realizam as tarefas de alguma instituição. Ainda segundo o autor, dois computadores estão interligados se eles são capazes de trocar informações.

Sousa (2013) afirma que uma boa infraestrutura de rede de computadores possibilita que empresas vendam mais, produzam mais e gerem mais empregos. Dentro das empresas, as tecnologias e equipamentos estão em constante evolução, sempre em busca da maior qualidade e menor índice de falhas, visando trazer ao usuário mais tranquilidade ao utilizar os equipamentos.

A comunicação entre os diversos equipamentos da rede se dá através de uma linguagem de comunicação denominada de protocolo. O estudioso define um protocolo de comunicação como um programa de computador, estabelecido através de regras pré-programadas, que permite a troca de dados entre dois locais, controlando seu envio e recepção, verificando erros, confirmando

recebimento, controlando o fluxo de dados, endereçando as mensagens, dentre outros aspectos.

2.2 Gerenciamento de Redes de Computadores

Basso (2020) afirma que com o crescimento da infraestrutura mundial das redes de computadores das empresas, o gerenciamento sistêmico desta enorme quantidade de componentes de hardwares e softwares se tornou muito importante. Com base no autor citado, ao montar uma rede com centenas ou milhares de componentes, é comum que alguns elementos sofram alguma sobrecarga, estejam mal configurados e parem de funcionar.

Comer (2016) define que um gerente de rede é a pessoa responsável pelo planejamento, instalação, operação, monitoramento e controle do hardware e software que constituem uma rede de computadores. Este planejamento deve atender aos requisitos mínimos de desempenho e seu monitoramento é essencial para observar se estes requisitos estão sendo atendidos, assim, detectando e corrigindo problemas que tornam a operabilidade da rede ineficiente.

O gerenciamento de redes é dividido em cinco categorias, sendo elas a de falhas, a de desempenho, a de configuração, a de segurança e a de contabilização. Para Basso (2020) o protocolo SNMP possui um papel fundamental no gerenciamento de falhas e de desempenho, pois a partir dele podemos obter informações sobre problemas que estão acontecendo e ainda medir o desempenho através de informações como tráfego utilizado, taxa de utilização de processamento, dentre outros.

2.3 Arquiteturas de Monitoramento

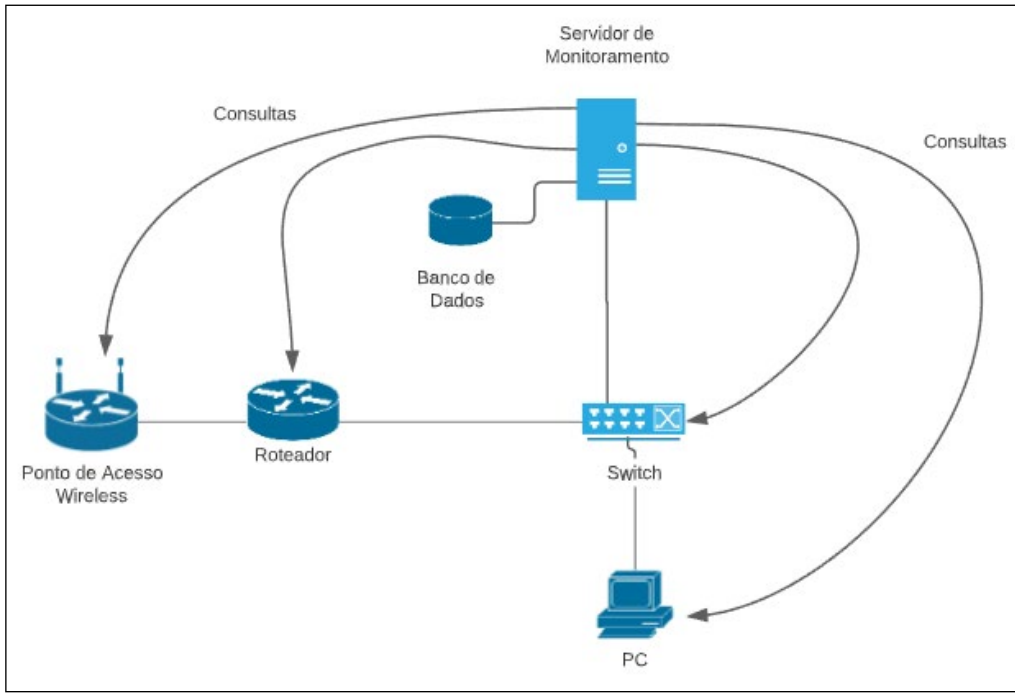
Um sistema para monitoramento de ativos de rede pode fazer uso de diferentes arquiteturas. Leinwand (1996) as classifica em três principais: Centralizada; Hierárquica; Distribuída. Apresentadas nas próximas subseções.

2.3.1 Arquitetura Centralizada

Leinwand (1996) diz que esse tipo de arquitetura tem apenas um servidor responsável por todo monitoramento da rede, utilizando apenas uma base de dados. Para obter plena redundância, este sistema deve realizar uma cópia de segurança para outro servidor em intervalos regulares, porém o foco do monitoramento da rede é o sistema principal.

Leinwand (1996) constata que o fato de haver apenas um local de monitoramento aumenta o consumo de banda em todos os links de rede ligados a este servidor, pois as consultas realizadas, para toda a rede, partem dali, conforme exemplificado na Figura 1.

Figura 1: Arquitetura de monitoramento centralizada



Fonte: adaptado de Leinwand (1996, p.22), pelo autor (2021).

Para Leinwand (1996) o uso de uma arquitetura centralizada é útil para a verificação e correlação entre problemas pois todos os dados de alertas e eventos estão localizados no mesmo local, assim, também providencia conveniência, acessibilidade e segurança para o administrador da rede. Porém, ter todo o monitoramento da rede num único ponto torna o sistema tolerante a falhas, já que não há redundância.

2.3.2 Arquitetura Hierárquica

Segundo Leinwand (1996), um sistema de monitoramento com uma arquitetura hierárquica faz uso de diferentes servidores, sendo que um trabalha como central e os outros como clientes, assim, algumas funcionalidades são executadas pelo servidor central e outras são distribuídas pelos clientes.

Nesse tipo de arquitetura os clientes não possuem uma base de dados própria, tendo que se comunicar com o servidor central para armazenar os registros obtidos, portanto, é necessária uma cópia de segurança desta base para garantir sua redundância.

Para Leinwand (1996) este tipo de abordagem ajuda a aliviar os problemas de uso de banda vistos na arquitetura centralizada, distribuindo tarefas de monitoramento entre o sistema central e seus clientes.

2.3.3 Arquitetura Distribuída

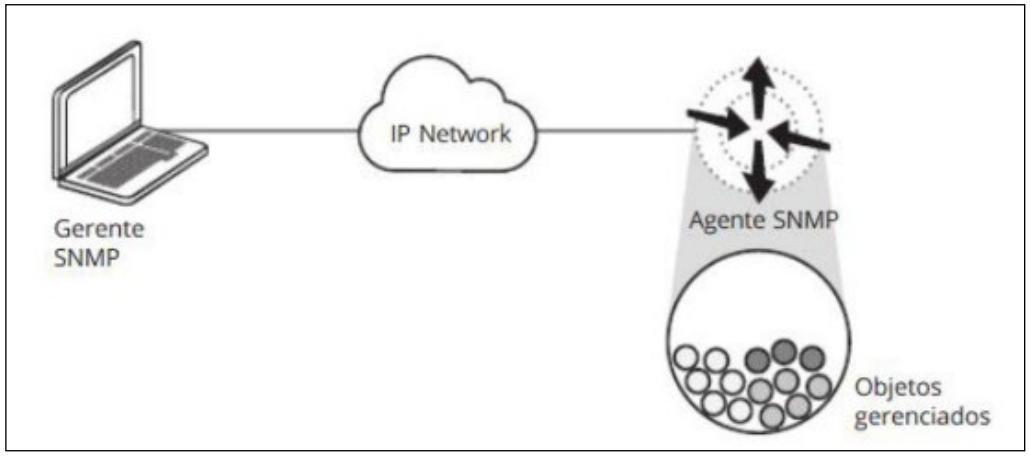
Segundo Leinwand (1996), a arquitetura distribuída combina a arquitetura centralizada e a hierárquica. Neste, o monitoramento da rede é espalhado em diversos servidores e cada um possui os dispositivos para monitorar e tem sua base de dados própria. A base de dados de cada servidor é replicada entre os diversos nós de monitoramento, garantindo que os dados não sejam perdidos caso algum deles estrague.

Leinwand (1996) constata que por combinar as duas arquiteturas anteriores, suas vantagens também são incluídas, como a de ter um único local para todas as informações, alertas e eventos da rede, não depender de um sistema único e a distribuição das tarefas de monitoramento pela rede.

2.4 Protocolo de Monitoramento SNMP

Branco (2015) diz que o protocolo padrão mais simples usado para gerenciamento de redes, adotado por vários fabricantes e operadores, é o SNMP. Segundo Basso (2020), as informações deste protocolo são trocadas entre uma entidade gerenciadora e um agente, sendo este último, presente no dispositivo gerenciado, comunicação apresentada na Figura 2.

Figura 2 - Modelo de comunicação SNMP



Fonte: Basso (2020, p. 18) apud Santos (2015).

Basso (2020) diz que o gerente coleta informações e controla as ações dos agentes, num trabalho conjunto, sendo responsável pela geração de relatórios e execução de atividades mais complexas.

Branco (2015) define o agente como entidade localizada perto do item gerenciado, como por exemplo, um switch, e ele responde às solicitações do

gerente via rede. O agente deve manter as informações de gerenciamento locais como um reflexo da realidade do equipamento gerenciado.

Basso (2020) aponta algumas características do protocolo SNMP são: protocolo aberto, utiliza o padrão Protocolo de Controle de Transmissão (*Transmission Control Protocol* - TCP) sobre Protocolo de Internet (*Internet Protocol* - IP), poucas operações, busca, armazenamento, é um protocolo da camada de aplicação, utiliza o Protocolo de Datagrama de Usuário (*User Datagram Protocol* - UDP) na camada de transporte e tem por padrão o uso das portas de comunicação 161 e 162. Por fazer uso do protocolo UDP, sua utilização realiza uma carga menor da rede.

2.4.1 SNMP versão 2

Segundo Basso (2020) a versão SNMP versão 2 veio para resolver algumas limitações da versão anterior, como a possibilidade de novos tipos de dados, macros, facilidades na transferência de grandes quantidades de dados, códigos de erros mais detalhados, melhoria em tabelas e novos grupos na Base de Informações de Gerenciamento (*Management Information Base* - MIB).

As operações que esta versão do protocolo pode realizar são:

- GetRequest - onde o gerente solicita informação ao agente;
- GetNextRequest - onde o gerente solicita a próxima variável da MIB do agente;
- SetRequest - onde o gerente define alguma informação no agente;
- GetBulkRequest - onde o gerente solicita uma grande quantidade de informação ao agente;
- InformRequest - onde um gerente informa outro sobre informações de uma MIB que é remota ao recebedor;
- Trap - onde o agente notifica ao gerente o acontecimento de alguma coisa.

2.4.2 SNMP versão 3

Na versão 3 do protocolo SNMP, Basso (2020) diz que ela trouxe uma série de melhorias de segurança, como autenticação e privacidade de comunicação entre a entidade gerenciadora e o agente. Além disso, segundo o autor, também foi introduzido um conceito chamado de MIB View, onde cada usuário pode acessar apenas as partes da MIB em que possui permissão.

Apesar do protocolo SNMP versão 3 trazer mais segurança, a versão 2c foi utilizada neste trabalho por estar disponível em uma quantidade maior de equipamentos.

2.4.3 Management Information Base

Kurose e Ross (2013) falam que os módulos MIB são especificados por padrões internacionais ou por fabricantes de equipamentos, sendo que a estrutura internacional é publicada pela Organização Internacional de Normalização (*International Organization for Standardization* - ISO).

Comer (2016) diz que o fato de o protocolo SNMP não especificar um conjunto de variáveis MIB, torna o projeto flexível, visto que novas variáveis MIB podem ser definidas e padronizadas conforme a necessidade. O autor complementa, ainda, que o mais importante é que a separação do protocolo de comunicação da definição dos objetos permite que qualquer grupo defina suas variáveis MIB conforme necessário.

Kurose e Ross (2013) dizem que os objetos são classificados obedecendo uma hierarquia, como se fosse uma árvore e cada ponto de ramo possui um nome e um número, com isso é possível identificar qualquer ponto da árvore pela sequência de nomes ou números especificados desde a raiz até o ponto desejado.

2.4.4 Segurança no protocolo SNMP

Segundo Mauro (2001), o protocolo SNMP v1 e v2 fazem uso da notação de comunidades para estabelecer a comunicação entre gerentes e agentes. Nos agentes existem três comunidades distintas para configurar, as de apenas leitura, de leitura e escrita e a de *trap*. Essas comunidades acabam se tornando basicamente as senhas de conexão entre gerente e agente.

Segundo Mauro (2001) a grande maioria dos fabricantes de equipamentos enviam seus produtos com comunidades SNMP padrões, sendo *public* para a comunidade de apenas leitura e *private* para leitura e escrita. Antes de disponibilizar um dispositivo na rede, é importante realizar a troca dessa configuração padrão.

Mauro (2001) diz que o maior problema de segurança encontrado nas primeiras duas versões do protocolo SNMP se encontra no fato de que as comunidades são enviadas entre gerentes e agentes como texto puro, não possuindo nenhum tipo de criptografia. Com isso, qualquer interceptador de dados consegue obter acesso ao nome da comunidade SNMP ao ter acesso aos pacotes de rede com esta informação. Para ajudar a contornar este problema, alguns equipamentos permitem que sejam definidos os endereços IPs que podem realizar requisições SNMP, ignorando as requisições dos que não estão na lista.

Partindo desta vulnerabilidade, o protocolo SNMPv3 surgiu para trazer mais segurança. Mauro (2001) menciona que esta versão do protocolo não trouxe grandes mudanças, além da adição de criptografia na comunicação.

Neste protocolo, a conexão entre gerente e agente acontece através de usuário e senha, que traz ainda mais segurança na comunicação.

3 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo são descritas a metodologia deste trabalho, os procedimentos técnicos e a forma de abordagem.

O caráter qualitativo desta pesquisa se realizou através da entrega de um panorama geral da rede monitorada, possibilitando o entendimento sobre quais pontos estão mais sobrecarregados, horários com maior uso e problemas mais recorrentes.

Já a parte quantitativa se deu através da plotagem de gráficos das informações coletadas pelo sistema, fornecendo uma fácil visualização dos dados reais de utilização da rede e dos equipamentos conectados, como computadores, switches, impressoras, entre outros.

O presente trabalho utilizou o método experimental para seu desenvolvimento. Sendo experimental por realizar o experimento da coleta de informações via protocolo SNMP, manipulando os parâmetros de como se dará esta coleta, através da escolha dos ativos e itens monitorados, visando identificar problemas relacionados com a infraestrutura de rede, computadores e serviços.

4 DESENVOLVIMENTO

Neste capítulo é apresentado os requisitos levantados para a implementação do sistema, bem como a descrição da base de dados criada e os casos de uso da ferramenta.

Segundo Kerr (2015) os requisitos funcionais demonstraram de forma clara as tarefas que o sistema deve contemplar do ponto de vista dos usuários. Kerr (2015, p. 21), diz que "os requisitos não funcionais referem-se a características globais do software, a critérios que qualificam os requisitos funcionais e aplicam-se ao sistema como um todo."

Visando oferecer um sistema de monitoramento de fácil utilização e que atenda as necessidades de um administrador de rede, foram levantados os requisitos funcionais e não funcionais mostrados no Quadro 1.

Quadro 1: Requisitos funcionais e não funcionais da aplicação

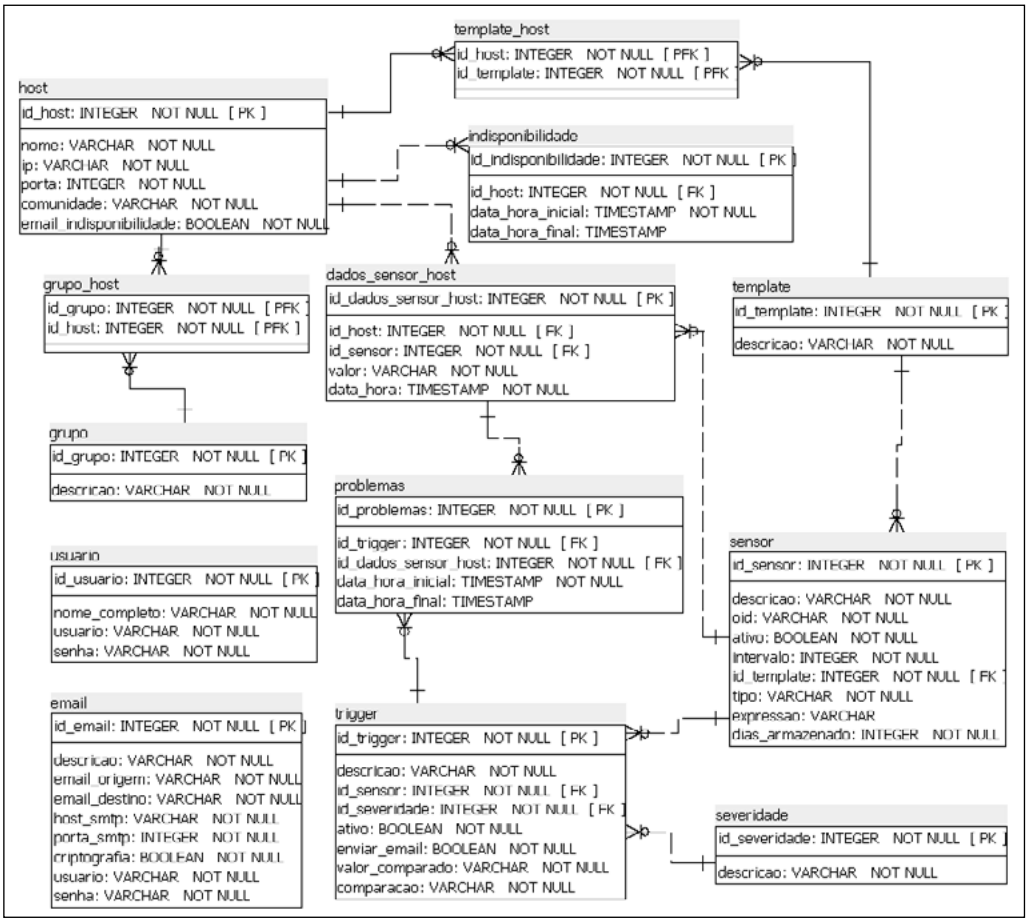
RF 1 - Manter cadastro de usuários Permitir cadastro, edição e exclusão de usuários
RF 2 - Manter cadastro de *hosts* Permitir cadastro, edição e exclusão de *hosts*
RF 3 - Manter cadastro de *templates* Permitir cadastro, edição e exclusão de *templates*
RF 4 - Manter cadastro de sensores Permitir cadastro, edição e exclusão de sensores
RF 5 - Manter cadastro de *triggers* Permitir cadastro, edição e exclusão de *triggers*
RF 6 - Manter cadastro de grupos de *hosts* Permitir cadastro, edição e exclusão de grupos de *hosts*
RF 7 - Permitir login com usuário e senha O sistema deve permitir apenas o acesso ao sistema dos usuários cadastrados com usuário e senha
RF 8 - Permitir visualização de dados coletados por gráficos O sistema deve permitir que qualquer sensor que possua informações numéricas seja visualizado em um gráfico de área. O usuário poderá escolher o intervalo dos dados entre 1 hora, 3 horas, 6 horas, 1 dia ou o período que quiser
RF 9 - Mostrar um panorama geral sobre os *hosts* O sistema deve exibir um panorama geral sobre os *hosts* da rede, informando quantos estão ativos, quantos estão inativos, problemas atuais e problemas encontrados nas últimas 3 horas. Também deve ser possível exibir este panorama agrupado por algum grupo de *hosts*
RF 10 - Mostrar relação de problemas encontrados em determinado período de tempo O sistema deve exibir um histórico dos problemas encontrados em determinado *host*, grupo de *hosts*, ou todos *hosts* da rede em um período de tempo escolhido pelo usuário
RF 11 - Cadastrar informações sobre e-mail O sistema deve permitir que o usuário defina as informações sobre o e-mail de envio e recebimento dos alertas
RF 12 - Alterar interface entre modo claro e escuro O sistema deve permitir que o usuário defina o modo de exibição da interface gráfica entre os modos claro e escuro
RF 13 - Permitir teste de consulta SNMP O sistema deve permitir que o usuário teste o resultado obtido em uma consulta SNMP no cadastro do sensor
RNF 1 - Ser compatível com o protocolo SNMP versão 2c O sistema deve ser capaz de se comunicar com os equipamentos da rede através do protocolo SNMP versão 2c

RNF 2 - Ser compatível com o navegador Google Chrome A aplicação web deve funcionar utilizando o navegador Google Chrome
RNF 3 - Ter o PostgreSQL como banco de dados O armazenamento dos dados obtidos deve ser realizado utilizando o PostgreSQL
RNF 7 - Ser desenvolvido em React e NodeJS O sistema deve ser desenvolvido utilizando React e NodeJS
RNF 5 - Permitir acessos simultâneos O sistema deve permitir no mínimo 15 acessos simultâneos
RNF 6 - Consultar sensores com base no período informado pelo usuário O sistema deve coletar as informações dos sensores cadastrados automaticamente com base no período informado pelo usuário
RNF 7 - Enviar notificações de *triggers* por e-mail O sistema deve enviar um e-mail ao usuário caso alguma *trigger* seja ativada, com os dados do *host*, do problema, data e hora da ocorrência
RNF 8 - Exclusão de dados antigos O sistema deve excluir automaticamente os dados com data anterior ao período escolhido pelo usuário no cadastro de sensor para mantê-los.
RNF 9 - Utilizar JWT para autenticar o usuário O sistema deve utilizar JWT para a autenticação do usuário em rotas protegidas, não podendo retornar dados em requisições não autenticadas.

Fonte: Elaborado pelo autor (2021).

Para representar o modelo do banco de dados que oferece uma maneira fácil de representar os dados que são salvos no sistema, foi criado o modelo Entidade-Relacionamento (ER) do banco de dados conforme a Figura 3, que atende aos requisitos definidos para o sistema.

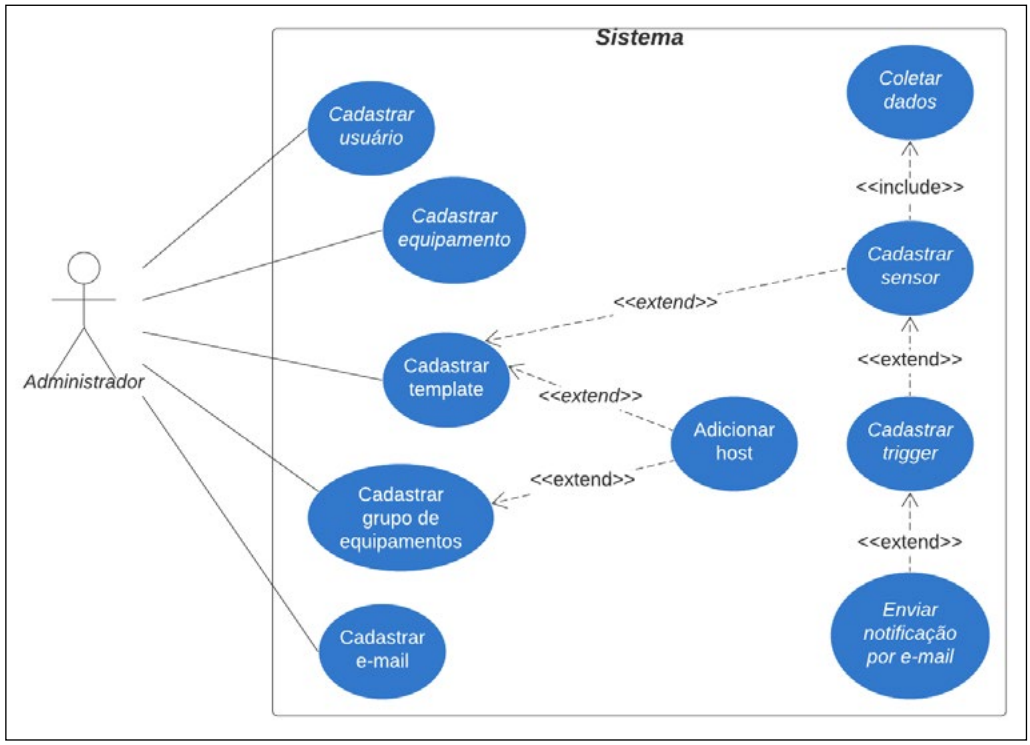
Figura 3: Modelo ER do banco de dados



Fonte: Elaborado pelo autor (2021).

Visando demonstrar de maneira fácil o comportamento do sistema ao reagir às ações feitas pelos atores, foi criado o diagrama de casos de uso, conforme mostrado na Figura 4.

Figura 4: Diagrama de casos de uso



Fonte: Elaborado pelo autor (2021).

5 TESTES E ANÁLISE DOS RESULTADOS

Neste capítulo são apresentados os testes realizados por meio da utilização da ferramenta, buscando apurar o correto funcionamento do monitoramento da rede por meio da comparação dos resultados apresentados no sistema com o estado real dos equipamentos.

5.1 Testes da ferramenta

Primeiramente, foi testada a capacidade da ferramenta de obter as informações pelo protocolo SNMP através do endereço IP, porta de comunicação e a comunidade SNMP de um switch HP 1920. Ao definir a informação de localização no equipamento, a ferramenta teve que a ler corretamente neste primeiro teste.

Este teste foi executado com sucesso pela ferramenta. No equipamento a localização foi atribuída como “Andar Superior”, mesma informação que o sistema apresentou em sua leitura.

Após êxito na consulta de informações, foi testada a automatização da coleta de dados, assim foi verificado se o sistema realiza as consultas no tempo estipulado e armazena as informações corretamente. Para isso foi cadastrado o switch HP 1920 utilizado no teste anterior e um template com o sensor de localização ativado para coleta a cada 30 minutos.

Ao deixar o sistema executando as suas consultas por aproximadamente 4 horas, foi executada uma consulta para ver se os dados estavam corretos e disponíveis, com isso foi verificado que o sistema coleta e armazena os dados corretamente.

Posteriormente, foram testados os alertas definidos no sistema, verificando se na ocorrência de determinado evento o sistema consegue perceber isto e encaminhar mensagens de e-mail ao usuário.

Para isso foi adicionado um gatilho para verificar se o consumo de rede da porta *trunk* de um switch HP 1920 ultrapassa os 15 Mbps. Ao deixar o sistema monitorando esta ação, foram recebidos diversos e-mails informando este acontecimento em diferentes horários, executando este teste com sucesso.

Também foi realizado um teste para verificar se os cálculos realizados em cima do retorno das consultas são executados corretamente. Para isso foi cadastrada uma impressora Samsung ML-3750nd, que ao buscar dados do Identificador de Objeto (*Object Identifier* - OID) 1.3.6.1.2.1.43.11.1.1.9.1.1, representando o nível de toner restante, retorna um valor entre 0 e 15.000. Visando obter um percentual de 0 à 100, foi aplicado o seguinte cálculo: retorno / 15000 * 100. Ao executar as consultas, o valor registrado foi transformado com base no cálculo corretamente.

Por fim, foi realizado um teste para verificar se o consumo de banda de um equipamento é apresentado corretamente pelo sistema. Para isso, foi cadastrado um sensor que representa a quantidade de bits recebidos na porta de internet de um servidor linux, comparando o que é apresentado no sistema criado e no sistema de configuração do próprio servidor.

Ao comparar o que foi apresentado pelo servidor linux, e o que foi gerado pelo sistema de monitoramento para o mesmo tráfego, foi percebido que o sistema desenvolvido se mostra competente ao buscar os dados e apresentá-los ao usuário, representando a velocidade real de uso de banda do equipamento monitorado.

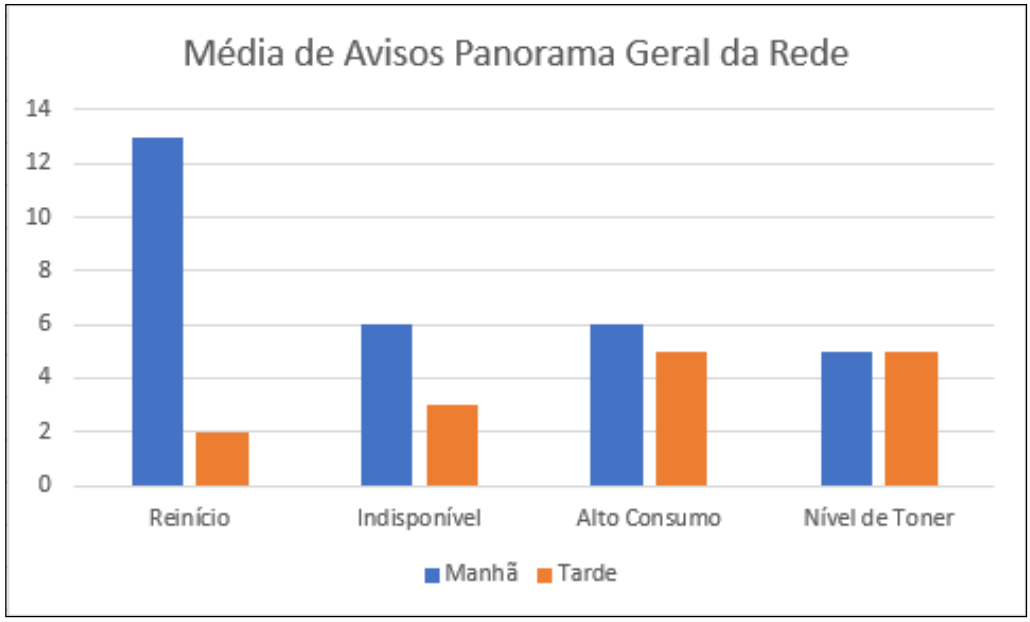
5.2 ANÁLISE DOS RESULTADOS

Para a realização da análise dos resultados obtidos através do uso da ferramenta desenvolvida, foram cadastrados 39 equipamentos, sendo 10 *switches* e 29 impressoras, que foram monitorados do dia 12 de abril de 2021 até 24 de maio de 2021. Estes equipamentos estavam dispersos em dez prédios municipais, conectados através de uma rede virtual privada.

5.2.1 Panorama da rede

Ao visualizar o panorama geral da rede foi verificado que muitos alertas são exibidos pelo fato de ter impressoras desligadas, com nível de toner baixo ou que tenham sido reiniciadas e isso pode tirar o foco do administrador sobre os problemas mais graves, principalmente no turno da manhã, que é quando as impressoras estão desligadas e são iniciadas, permanecendo os avisos no histórico dos problemas encontrados nas últimas três horas do panorama, conforme apresentado no Gráfico 1.

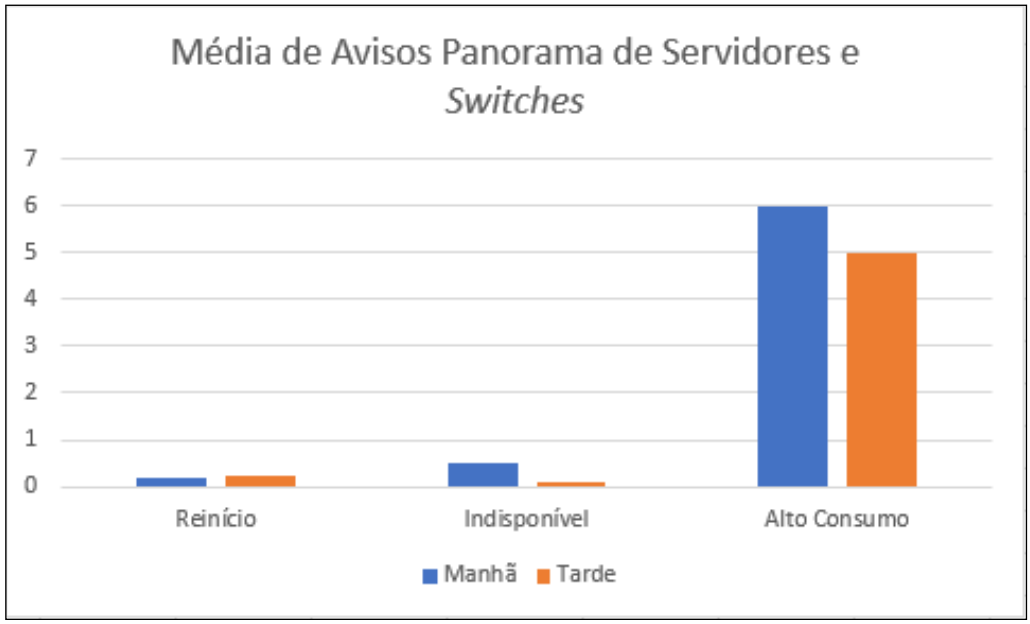
Gráfico 1: Média alta de avisos no panorama geral da rede



Fonte: Elaborado pelo autor (2021).

Ao segmentar o panorama por algum grupo específico de equipamentos, o mesmo representa apenas o grupo, não contendo informações de outros equipamentos. Com isso, é possível visualizar apenas os avisos e problemas dos equipamentos, que são os mais importantes. No Gráfico 2 é demonstrada a média de problemas e avisos do grupo de servidores e switches, equipamentos essenciais para o funcionamento da rede.

Gráfico 2: Média baixa de avisos no panorama de servidores e switches



Fonte: Elaborado pelo autor (2021).

Ao comparar os gráficos do panorama geral e o de servidores e switches podemos verificar que a visualização dos problemas mais importantes se torna mais fácil ao utilizar a segunda forma, já que mostram apenas as coisas relacionadas ao grupo, exibindo em média 12,05 itens num dia, e no geral em média 45 itens.

Ambos apresentam o estado atual dos equipamentos de maneira correta, porém o panorama geral apresenta avisos e problemas que podem não impactar a experiência dos usuários.

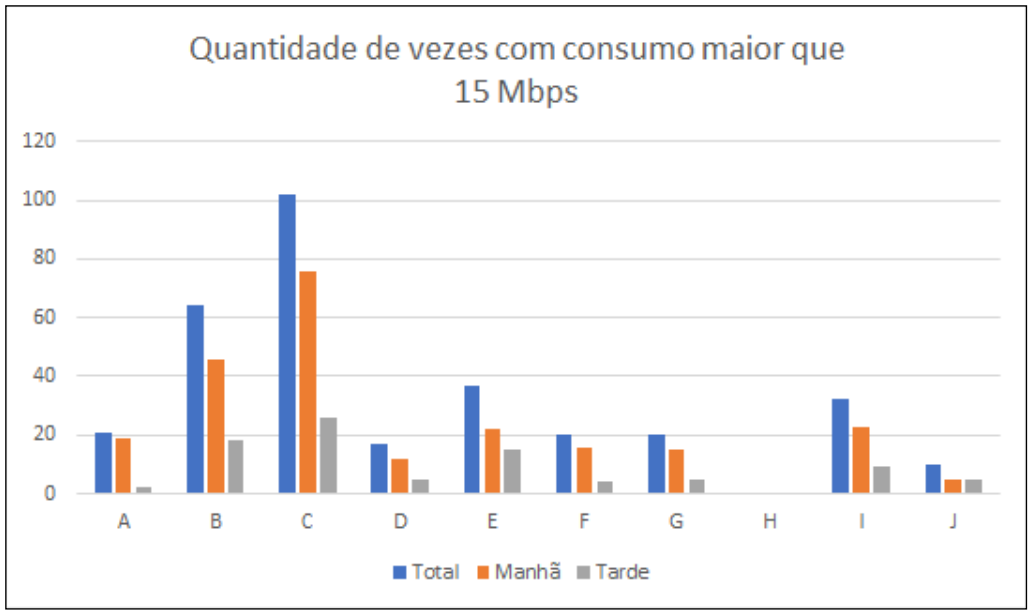
5.2.2 Pontos com maior consumo de banda

Para verificar os pontos com maior consumo de banda por local, foi adicionado um gatilho para avisar quando algum switch ultrapassa 15 Mbps (Megabits por segundo) de consumo médio na porta *trunk*, que é a responsável por disponibilizar a rede interna e internet para cada prédio. Por exemplo, a porta *trunk* do switch principal do local 'A' entrega a rede interna e internet para todos os equipamentos deste mesmo lugar, sendo ela a responsável por todo o tráfego do mesmo, exceto a comunicação entre os dispositivos dele.

Por meio da ferramenta, foi possível verificar quais pontos tiveram maior consumo de rede. Como demonstrado no Gráfico 3, o local C possui o maior consumo, visto que ultrapassou os 15 Mbps de uso 102 vezes, seguido pelo local 'B' ultrapassando este consumo 64 vezes. Além disso, é possível

identificar que o período com maior consumo é o da manhã, estando à frente em 8 dos 10 locais.

Gráfico 3: Vezes em que os locais ultrapassaram 15 Mbps de consumo de rede



Fonte: Elaborado pelo autor (2021).

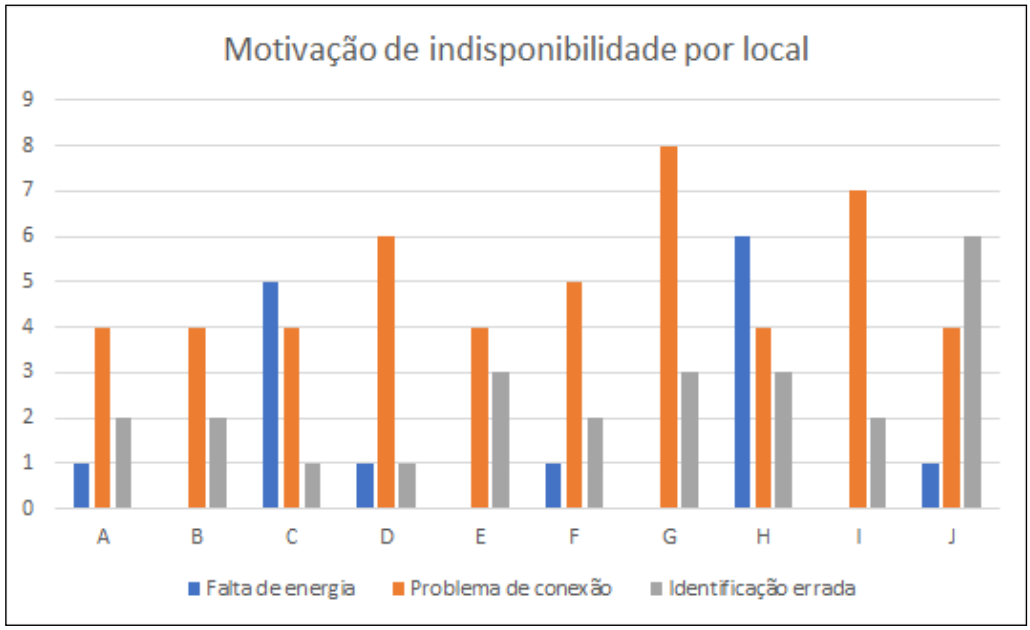
5.2.3 Correlação entre os avisos de indisponibilidade e seus motivos

Para verificar se a ferramenta identifica corretamente os momentos de indisponibilidade dos dispositivos, foram analisados os resultados obtidos através do histórico de problemas encontrados em comparação com os acontecimentos reais dos equipamentos. Esta análise foi feita sobre os switches espalhados entre diversos locais, buscando identificar problemas de conexão, queda de energia ou identificação errada de indisponibilidade pela ferramenta.

Ao analisar os resultados apresentados no Gráfico 4, é possível concluir que os locais 'G' e 'I' apresentaram os maiores problemas de conexão no período, 8 vezes no primeiro e 7 no outro.

Além disso, é possível verificar que os pontos 'H' e 'C' possuem uma maior instabilidade na energia elétrica, causando a perda de conexão e reinício dos aparelhos. No ponto 'H' a energia caiu 6 vezes, enquanto no ponto 'C', 5.

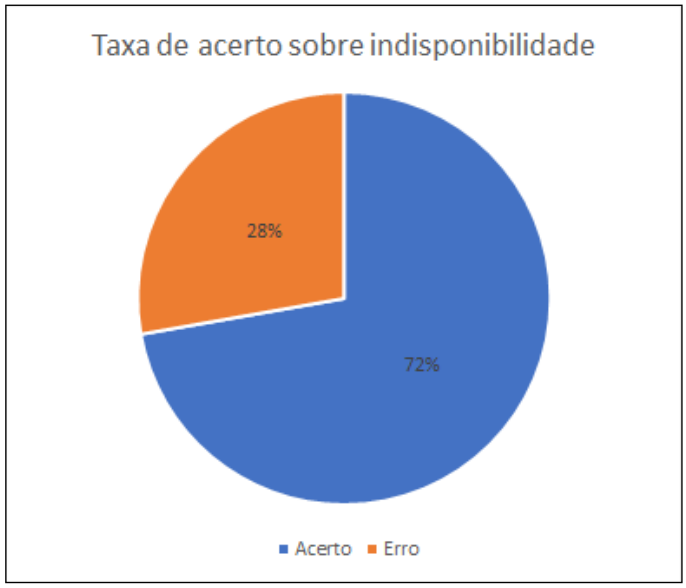
Gráfico 4: Motivação de indisponibilidade por local



Fonte: Elaborado pelo autor (2021).

Já o Gráfico 5, que auxilia a visualização da taxa de acerto sobre o gráfico anterior, mostra que a ferramenta apresenta indisponibilidade de equipamentos erroneamente com certa frequência, e isso pode atrapalhar o serviço dos administradores de rede, visto que podem parar algum trabalho para corrigir um problema inexistente.

Gráfico 5: Taxa de acerto sobre indisponibilidade em switches



Fonte: Elaborado pelo autor (2021).

5.2.4 Problemas identificados no grupo de impressoras

Para a análise dos problemas relacionados ao grupo de impressoras monitoradas, foram adicionados gatilhos no sistema para alertar quando alguma impressora fique indisponível, reinicie ou fique com um nível de toner abaixo de 5%. Após isto, foram anotados todos os chamados relacionados a problemas com as impressoras, comparando os problemas relatados e os alertas ativos no momento.

Concluiu-se que há muitos momentos de indisponibilidade e reinício dos equipamentos. Isso é devido ao desligamento das impressoras no intervalo do meio dia e final de expediente em muitas delas, o que levou a alta taxa de avisos do tipo. É importante ressaltar que cada reinício leva também a mais um momento de indisponibilidade, pois ao reiniciar alguma impressora a mesma fica indisponível neste mesmo período de tempo, ou seja, foram 106 avisos de indisponibilidade por falha de comunicação, seja ela queda na rede ou equipamento com o cabo de rede desconectado, ou identificação errada de indisponibilidade.

Visando o verificar o auxílio da ferramenta em chamadas de suporte, está constatado que todas as vezes onde havia um apontamento de alguma impressora indisponível, ela realmente não estava acessível para impressão, estando desligada, com mal contato ou desconectada do cabo de rede, obtendo 100% de sucesso ao auxiliar o suporte.

Visualizando os resultados obtidos através dos alertas sobre o baixo nível restante de toner das impressoras, é possível concluir que o sistema emite alertas quando alguma impressora começa a ficar sem toner, auxiliando o suporte em chamados onde a questão surge de impressões fracas, com uma taxa de acerto de 87,5%. Na ocasião em que errou, foi visto que ao trocar o toner da impressora o nível restante apontado caiu para -2 em vez de voltar a 100. Ao analisar a causa disso, foi visto que ao inserir um cartucho recarregado sem os devidos ajustes, a impressora quer informar com o valor -2 que não é possível indicar o nível restante do toner, assim o sistema fica alertando para a falta de toner.

6 CONSIDERAÇÕES FINAIS

Uma boa gerência de redes de computadores e equipamentos é essencial para o bom funcionamento da mesma. Um local em que seus dispositivos funcionem corretamente, agrega agilidade e qualidade ao serviço prestado, além de dar mais tranquilidade e satisfação aos usuários.

Ao passo do crescimento do uso da tecnologia, as redes de computadores cada vez se tornam maiores e mais complexas, exigindo um acompanhamento sistêmico de seus administradores, visto que analisar manualmente cada ponto da rede acaba por tomar muito tempo, algo muito valioso nos dias atuais.

Esta situação trouxe a indagação sobre como um sistema de monitoramento de ativos de rede consegue auxiliar administradores de rede a resolver problemas e como ele consegue prever que algum problema possa vir a acontecer.

Visando resolver o problema foi desenvolvida uma ferramenta para auxiliar os administradores da rede dos prédios municipais de Arroio do Meio, Rio Grande do Sul, a monitorar os diversos equipamentos utilizados, objetivando identificar por meio da ferramenta problemas na rede, diminuir a ocorrência de problemas, auxiliar na resolução de problemas e melhorar os atendimentos em chamadas de suporte.

O uso da ferramenta resultou em um monitoramento ativo de 39 equipamentos e conforme os resultados apresentados na análise, ela atingiu seus objetivos. Ao alertar os administradores sobre alto consumo de banda em determinados locais, a ferramenta conseguiu identificar problemas ocorridos na rede e com estes dados os administradores puderam dimensionar a capacidade de cada local variando com a necessidade, o que propiciou a diminuição de problemas.

Já, ao alertar os administradores sobre o baixo nível de toner restante nos equipamentos, os administradores ficavam cientes do problema que viria a acontecer, que é a má qualidade de impressão. Com isso, a ferramenta atingiu o objetivo de auxiliar na resolução de problemas, além de prever que algum problema venha a acontecer.

Ao alertar a indisponibilidade de equipamentos na rede, a ferramenta demonstrou problemas ao identificar aparelhos indisponíveis em momentos que estavam funcionando, o que pode levar a perda do foco em situações mais importantes.

De uma forma geral ficou visível a necessidade da utilização de um sistema de monitoramento de ativos de rede, vista a necessidade de seu bom funcionamento. Um sistema destes facilita o monitoramento de ativos, já que o faz de forma automatizada, requerendo apenas os cadastros de equipamentos, sensores e gatilhos. Além disso, ele melhora o atendimento em chamadas de suporte técnico, uma vez que dispõe de informações em tempo real do equipamento em que foi relatado o problema, o auxiliando em sua resolução.

REFERÊNCIAS

BASSO, Douglas E. **Administração de Redes de Computadores.** Curitiba: Contentus, 2020.

BRANCO, Kalinka R. L. C.; GURGEL, Paulo H. M.; BRANCO, Luiz H. C.; BARBOSA, Ellen F.; TEIXEIRA, Mário M. **Redes de Computadores:** Da teoria à prática com Netkit. 1. ed. Rio de Janeiro: Elsevier, 2015.

COMER, Douglas E. **Redes de Computadores e Internet.** Tradução de José V. de Lima e Valter Roesler. 6. ed. Porto Alegre: Bookman, 2016.

KEMP, Simon. **Digital 2021 Global Overview Report.** Disponível em: https://datareportal.com/reports/digital-2021-global-overview-report. Acesso em: 17 mar. 2021.

KERR, Eduardo S. **Gerenciamento de requisitos.** São Paulo: Pearson Education do Brasil, 2015.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** uma abordagem top-down. Tradução de Daniel Vieira. Revisão técnica de Wagner L. Zucchi. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

LEINWAND, Allan; CONROY, Karen F. **Network Management:** A Pratical Perspective. 2nd ed. Massachusetts, EUA: Addison-Wesley, 1996.

SOUSA, Lindeberg B. de. **Redes de Computadores:** Guia Total. 1. ed. São Paulo: Érica, 2013.

MAURO, Douglas R.; SCHMIDT, Kevin J. **Essential SNMP.** 1. ed. Califórnia, EUA: O'Relly & Associates, Inc., 2001.

TANENBAUM, Andrew S. **Computer Networks.** 3rd ed. Nova Delhi, India: Prentice Hall, 1996.