Disciplinarum Scientia. Série: Naturais e Tecnológicas, Santa Maria, v. 24, n. 2, p. 115-133, 2023.
Recebido em: 26.04.2023. Aprovado em: 06.10.2023.
ISSN 2176-462X
DOI: 10.37779/nt.v24i2.4534

GERENCIAMENTO DA REDE: INFRAESTRUTURA E MONITORAMENTO DO HOSPITAL UNIVERSITÁRIO DE SANTA MARIA (HUSM)

NETWORK MANAGEMENT: INFRASTRUCTURE AND MONITORING OF HOSPITAL UNIVERSITÁRIO DE SANTA MARIA (HUSM)

Rafael Geneves Porto Azambuja[1], Walter Priesnitz Filho[2], Simone Regina Ceolin[3], Rafael Teodósio Pereira[4] e Renato Preigschadt Azevedo[5]

RESUMO

A pesquisa relata as atividades realizadas no monitoramento de infraestrutura da Tecnologia de Informação, do Setor de Tecnologia da Informação e Saúde Digital (SETISD) do Hospital Universitário de Santa Maria (HUSM) da Universidade Federal de Santa Maria (UFSM), tendo como foco principal destas atividades, os requisitos levantados a partir da gerência do setor e também o contexto hospitalar. As técnicas de monitoramento de rede permitem aos gerentes da rede obter informações sobre o desempenho da rede e observar padrões sazonais e a identificação de falhas. Com isso, busca-se observar os problemas referente a topologia lógica da rede, através do monitoramento da mesma e a documentação da sua infraestrutura, tendo como objetivo principal do trabalho, tornar este monitoramento mais eficiente e automatizado possível, o trabalho realizado buscou tornar o sistema de monitoramento o mais eficiente e automatizado possível. As soluções implementadas durante a pesquisa e desenvolvimento quando comparadas com as que já existiam, apresentaram menor uso de recursos computacionais, notificações de alertas que ajudem a determinar com precisão a origem do problema e menor necessidade de configurações referentes ao cadastro e monitoramento de novos dispositivos.

Palavras-chave: Tecnologia da Informação, detecção de falhas.

ABSTRACT

The research reports the activities carried out in the monitoring of Information Technology infrastructure within the Information Technology and Digital Health Sector (SETISD) of the University Hospital of Santa Maria (HUSM) at the Federal University of Santa Maria (UFSM). The main focus of these activities is the requirements identified through departmental management and the hospital context. Network monitoring techniques enable network managers to gather information on network performance, observe seasonal patterns, and identify faults. As such, the goal is to address issues related to the logical network topology through continuous monitoring and documentation

1 Graduado em Tecnologia em Redes de Computadores (2023), no Colégio Técnico Industrial (CTISM) de Santa Maria, da Universidade Federal de Santa Maria. Atualmente, participa do grupo de pesquisa NERSEC do CTISM e aluno de graduação do curso de matemática da Universidade Federal de Santa Maria. E-mail: rafaelazambuja@redes.ufsm.br. ORCID: https://orcid.org/0009-0000-8372-8635

2 Professor Adjunto da Universidade Federal de Santa Maria - UFSM/CTISM. E-mail: walter@redes.ufsm.br. ORCID: https://orcid.org/0000-0002-8999-4843

3 Professora Associada II no Colégio Técnico Industrial da Universidade Federal de Santa Maria - UFSM/CTISM. E-mail: sceolin@redes.ufsm.br. ORCID: https://orcid.org/0000-0003-3750-2007

4 Professor Adjunto da Universidade Federal de Santa Maria, atuando na área de Redes de Computadores, com ênfase em Redes de Sensores sem Fio e Banco de Dados. E-mail: rafatp@redes.ufsm.br. ORCID: https://orcid.org/0000-0003-4901-1619

5 Professor adjunto da Universidade Federal de Santa Maria. E-mail: renato@redes.ufsm.br. ORCID: https://orcid.org/0000-0002-5045-9595

of its infrastructure. The primary objective of this work is to make this monitoring as efficient and automated as possible. The solutions implemented during the research and development phase, when compared to existing ones, showed reduced usage of computational resources, alert notifications that assist in precisely determining the source of problems, and reduced requirements for configuring the registration and monitoring of new devices.

Keywords: *Information Technology, fault identification.*

INTRODUÇÃO

A implantação de uma infraestrutura de rede vai além da interconexão física entre dispositivos. Os objetivos referentes à implementação de uma rede são alcançados através de planejamento quanto a configurações, equipamentos e tecnologias que dão forma à rede. Para Clemm (2006), o gerenciamento de rede é o conjunto de atividades, métodos, procedimentos e ferramentas que constituem a operação, administração, manutenção e provisionamento de sistemas em rede.

Uma infraestrutura de Tecnologia da Informação (TI) está intrinsecamente sujeita a falhas. As práticas de gerenciamento podem permitir ao gerente trabalhar de maneira proativa, notando padrões e indicativos de possíveis falhas que poderão ocorrer, e facilitando a identificação de falhas (CLEMM, 2006). O Setor de Tecnologia da Informação e Saúde Digital (SETISD) do Hospital Universitário de Santa Maria (HUSM) e suas unidades são responsáveis pela execução, implementação e manutenção de serviços de TI no âmbito hospitalar do HUSM. O SETISD-HUSM é responsável por propor, gerir, manter e apoiar soluções de Tecnologia da Informação e Saúde Digital no âmbito do hospital.

As unidades e cargos atribuídos possibilitam a identificação daqueles responsáveis pelas tomadas de decisão, permitindo que um novo funcionário, estagiário ou analista externo a obtenção de informações sobre a infraestrutura de rede e seus serviços.

O setor conta com funcionários da Empresa Brasileira de Serviços Hospitalares (EBSERH) e servidores do Regime Jurídico Único vinculados à Universidade Federal de Santa Maria para trabalhos relacionados à infraestrutura de TI, e funcionários de empresas terceirizadas para suporte técnico ao cliente interno e manutenção de equipamentos.

A infraestrutura de TI implantada pelo SETISD-HUSM contém diversos dispositivos e serviços. No âmbito hospitalar, um incidente na rede pode ocasionar graves consequências. O monitoramento da infraestrutura permite trabalhar de maneira proativa identificando falhas e permitindo que medidas sejam tomadas tão cedo quanto possível.

A automatização de ferramentas de monitoramento diminui a necessidade de manutenção das ferramentas de monitoramento quanto às alterações na rede, evitando por exemplo, problemas ocasionados pelo esquecimento da manutenção da ferramenta. A abordagem de tornar as soluções de monitoramento automatizadas refere-se à menor necessidade de intervenção humana para manutenção das ferramentas de monitoramento quanto às configurações de sondagem.

A implementação de uma solução de monitoramento vai além da implantação de uma ferramenta de monitoramento. A pesquisa e desenvolvimento torna o sistema de monitoramento eficiente, utilizando a menor quantidade de recursos computacionais possível, tornando a geração de incidentes mais precisa para identificação da origem do problema, evitando a geração de incidentes dependentes, automatizando as soluções de monitoramento, e visando menor número de configurações estáticas e menor necessidade de manutenção.

Para alcançar os objetivos quanto ao monitoramento da rede, foi necessário estabelecer os seguintes passos:

- Identificar os requisitos da gerência;
- Identificar os responsáveis pelas tomadas de decisão;
- Conhecer o modo de operação do setor e suas responsabilidades;
- Caracterizar a infraestrutura de TI, identificando: os principais servidores, equipamentos de rede, os serviços oferecidos e o método de documentação.
- Estudar as ferramentas de monitoramento propostas pelo setor: identificar como os recursos oferecidos pelas ferramentas podem ser utilizados no contexto do setor, buscar na bibliografia acadêmica as práticas e referências utilizadas no monitoramento de rede;
- Análise das ferramentas já existentes no setor: identificar as ferramentas utilizadas: analisar a lógica de monitoramento atual, analisar o desempenho das ferramentas, como impacto na rede e utilização dos recursos computacionais;
- Reestruturação do sistema de monitoramento;
- Análise das soluções implementadas e otimização;
- Apresentação das soluções aos funcionários;
- Correções com base no retorno dos funcionários;
- Comparação entre as soluções existentes com as soluções implementadas;
- Documentação das soluções implementadas;
- Proposta de melhorias.

GERENCIAMENTO DE REDE

A arquitetura do gerenciamento de rede é composta por dispositivos gerenciáveis, sistema de gerenciamento e protocolos de gerenciamento (KUROSE; ROSS, 2013). O sistema de gerenciamento, responsável pela sondagem, providencia as ferramentas para coleta, processamento e visualização de informações sobre os dispositivos gerenciados (KUROSE; ROSS, 2013).

Um dispositivo gerenciável é um elemento de rede que, através de um agente de gerenciamento, fornece uma interface de gerenciamento que possibilita a comunicação com o sistema de gerenciamento. O agente de gerenciamento também é responsável pela implementação de uma base

de informações de gerenciamento que representa uma coleção de objetos gerenciáveis, parâmetros e configurações referentes à *hardware* e *software*. Por fim, o agente também é responsável por implementar uma lógica para a relação entre a base de informações de gerenciamento e o dispositivo. A troca de mensagens entre o sistema de gerenciamento e o agente de gerenciamento através de um protocolo de gerenciamento ocorre em uma relação cliente-servidor, onde o agente atua como servidor, suprindo o sistema de gerenciamento com informações sobre seus objetos gerenciados (CLEMM, 2006).

A divisão do gerenciamento de rede em dimensões é uma maneira de permitir a divisão de problemas em diferentes aspectos, e assim, trabalhá-los sistematicamente (CLEMM, 2006).

O modelo conceitual *Fault, Configuration, Accounting, Performance, Security* (FCAPS) organiza as funções de gerenciamento que atuam sobre as camadas de gerenciamento, segundo Clemm (2006), da seguinte forma:

- O Gerenciamento de Falhas lida com questões relacionadas à indisponibilidade de recursos e usabilidade;
- O Gerenciamento de Configuração abrange as operações de leitura e escrita que garantem a implantação dos serviços de rede desejados;
- O Gerenciamento de Contabilidade aborda as questões de responsabilidade do uso da infraestrutura de rede;
- O Gerenciamento de Desempenho refere-se à análise dos indicadores de performance;
- O Gerenciamento de Segurança traz as práticas de proteção dos recursos da infraestrutura de TI.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Simple Network Management Protocol (SNMP) é um protocolo comumente utilizado para o gerenciamento de dispositivos IP. Os sistemas de gerenciamento se comunicam com dispositivos gerenciáveis que possuam um agente SNMP, no modelo Cliente/Servidor, através de mensagens SNMP solicitadas ou não solicitadas (MAURO, 2001).

Atualmente existem três versões do protocolo: SNMPv1, SNMPv2c e SNMPv3. A Figura 1 traz os pontos principais de cada versão. O protocolo possui os seguintes tipos de mensagem (MAURO, 2001):

- *Get-request*: mensagem enviada pelo sistema de gerenciamento para um agente SNMP, requisitando informações sobre um objeto gerenciável;
- *Get-next-request*: mensagem enviada pelo sistema de gerenciamento para um agente SNMP, requisitando um grupo sequencial de informações da MIB de um dispositivo gerenciável. Em outras palavras, as mensagens *Get-next-request* percorrem uma subárvore

de maneira lexicográfica até que o agente notifique o sistema de gerenciamento que não existem mais objetos subsequentes;

- *Get-bulk-request*: Definida na versão 2 do protocolo, permite a coleta de um volume maior de informações de uma única vez;
- *Get-response*: Resposta enviada pelo agente SNMP às requisições do sistema de gerenciamento;
- *Set*: Usada para alterar o valor de um objeto gerenciável e adicionar novas entradas;
- *Trap*: mensagens não solicitadas enviadas pelo agente SNMP para o sistema de gerenciamento para notificação de eventos, como mudança de estado em uma interface de rede;
- *Notification*: mensagens não solicitadas enviadas pelo agente SNMP para o sistema de gerenciamento para notificação de eventos. Definida na versão 2 do protocolo, é uma revisão das *Traps* SNMPv1;
- *Inform*: troca de mensagens entre sistemas de gerenciamento.

Figura 1 - Versões do protocolo SNMP.

Evolution of SNMP Standard

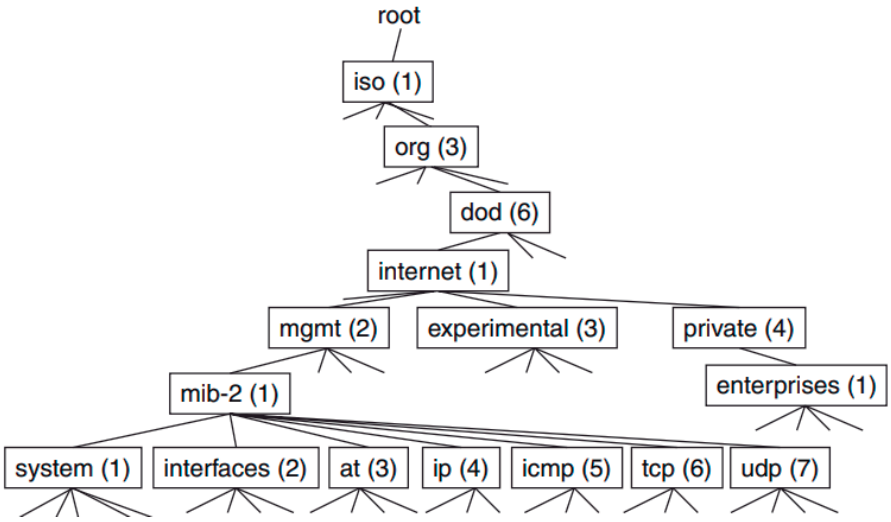
SNMP Version		RFC	Highlights
SNMPv1		1155, 1157, 1212	First SNMP implementation, used private and public community strings for security. Five operations: Get, Set, GetNext, Response, and Trap
SNMPv2	SNMPv2	1441–1452	Major improvements in performance with "GetBulk" and better security
	SNMPv2u	1909, 1910	Easier configuration
	SNMPv2*	IETF Draft	Remote configuration
	SNMPv2c	1901–1908	No remote configuration, uses community strings
SNMPv3		2271–2275	Takes most of the improvements from SNMPv2. Adds strong security and authentication model, support for remote agent configuration with SNMP, and unique ID for each SNMP engine

Fonte: (PHALTANKAR, 2000).

MANAGEMENT INFORMATION BASE (MIB)

A *Management Information Base* (MIB) é uma base conceitual de informações que oferece uma abstração do dispositivo gerenciável ao sistema de gerenciamento. As informações contidas em uma MIB são organizadas em uma árvore conceitual (Figura 2), onde cada nó é associado a uma sequência léxica de caracteres, denominada *Object Identifier (OID)*, que representa o caminho percorrido na árvore (CLEMM, 2006).

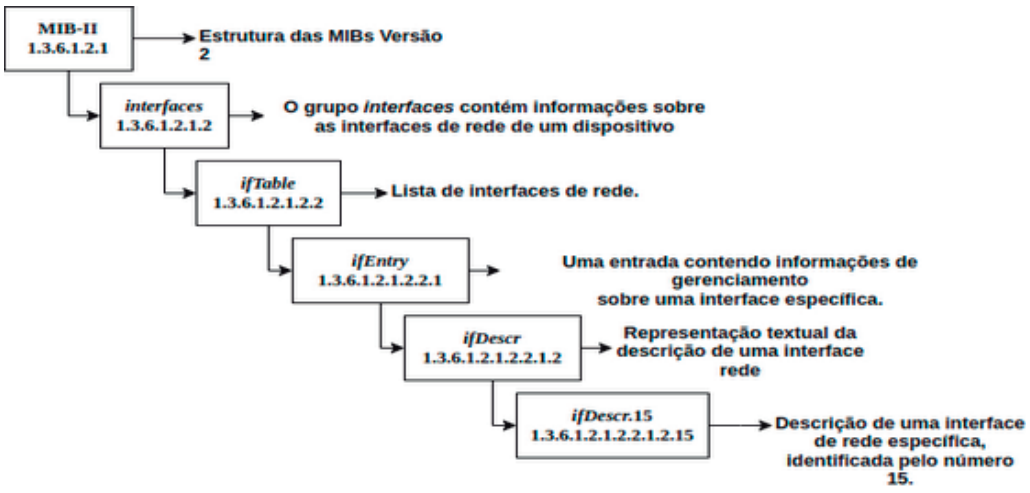
Figura 2 - Representação em forma de árvore.



Fonte: (CLEMM, 2006).

Por exemplo, a coleta de dados referentes à descrição de uma interface de rede identificada pelo índice '15', do objeto gerenciável ifDescr, pode ser feita utilizando a MIB-II, definida na RFC 1213. O objeto gerenciável utilizado para sondagem dessa informação é dado pela OID 1.3.6.1.2.1.2.2.1.2.15. O caminho para encontrar esta informação é representado pela Figura 3.

Figura 3 - Caminho até *ifDescr*.



Fonte: autor

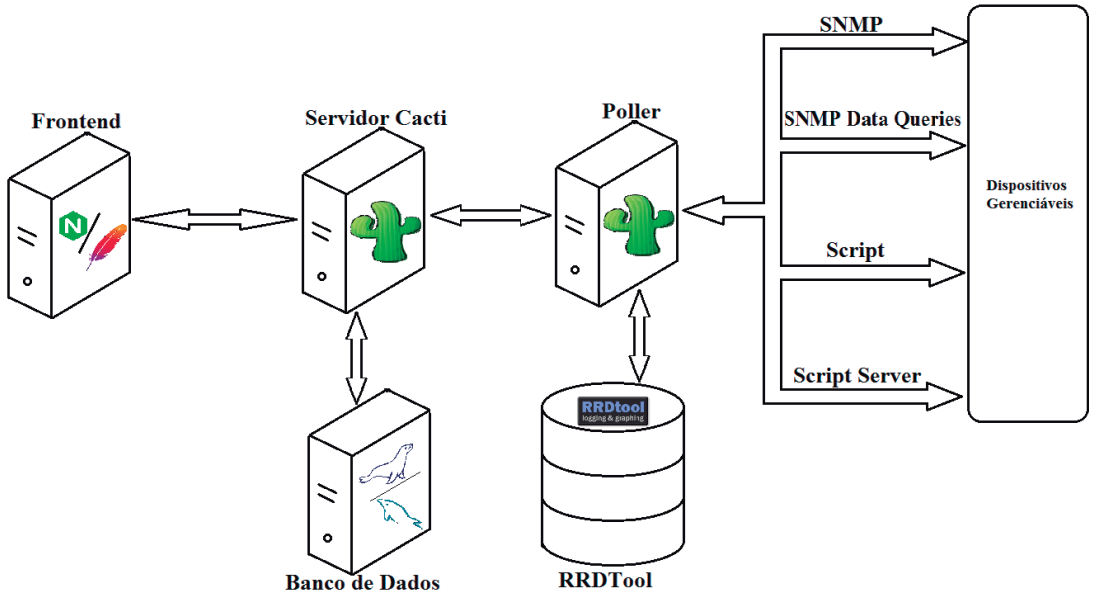
CACTI

O Cacti é uma ferramenta de monitoramento que atua como *frontend* do sistema *RRDTool*. O sistema *RRDTool* utiliza a técnica *Round Robin*, utilizando uma quantidade fixa de espaço de armazenamento. Quando todo espaço for utilizado, os dados mais antigos são substituídos pelos novos dados (BOGAERDT, 2022).

Inicialmente desenvolvido para Gerenciamento de Desempenho, hoje em dia o Cacti, nativamente ou com uso de *plugins*, pode contemplar o Gerenciamento de Falhas, *Backup* de configurações de roteadores, mapeamento de rede, etc (CACTI, 2023). A arquitetura do Cacti, representada pela Figura 4, é composta por:

- Servidor *Hypertext Transfer Protocol* (HTTP): fornece o *frontend* para o usuário;
- Banco de dados: armazenamento de configurações relacionadas à sondagem;
- *RRDTool*: armazenamento de séries temporais e construção de gráficos;
- Servidor Cacti: centralização do ecossistema do Cacti;
- *Poller*: Instâncias do Cacti responsáveis pela sondagem;
- *Data Input Methods*: método de coleta de dados, podendo ser:
  - SNMP: coletas que utilizam mensagens SNMP *Get*;
  - SNMP *Data Queries*: método de coleta que permite maior grau de customização e automatização. Fornece um meio para utilização de coletas através de mensagens SNMP *Get-next*;
  - *Scripts*: utiliza a saída de *scripts* externos como dado coletado. *Scripts* estendem a funcionalidade da coleta de dados do Cacti e podem ser escritos em quase qualquer linguagem (BERRY *et al.*, 2017).
  - *Script Queries*: *scripts* cuja saída é indexada;
  - PHP *Script Server*: Interpretador de PHP residente na memória utilizado para sondagem (BERRY *et al.*, 2017).

Figura 4 - Arquitetura do Cacti.



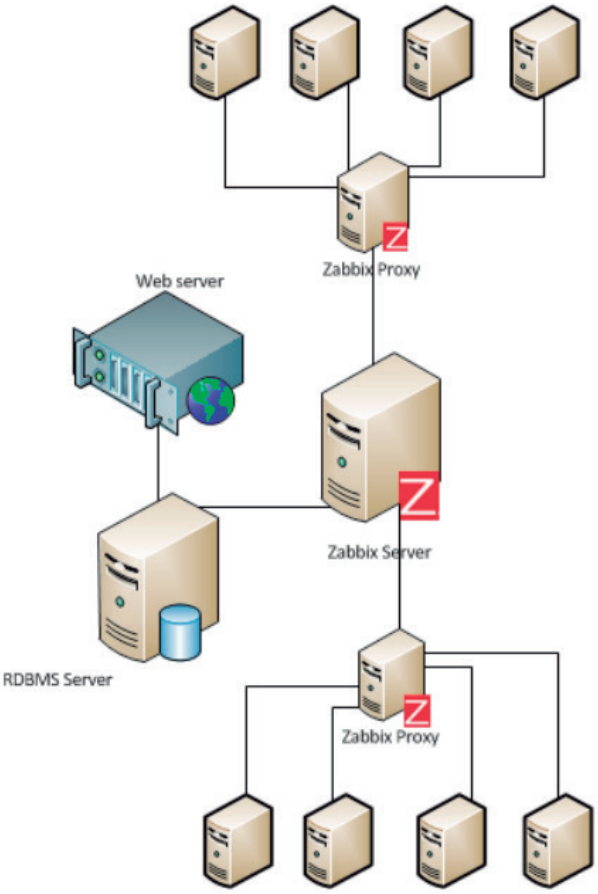
Fonte: Autor.

Para facilitar o monitoramento, o Cacti permite a criação de *templates*, moldes de configuração aplicados aos dispositivos cadastrados, gráficos e coleta de dados, e o recurso de descoberta de rede, para cadastro automático de dispositivos na rede.

ZABBIX

O Zabbix é uma ferramenta de monitoramento de rede que realiza coleta de dados através de diversos protocolos, constrói gráficos, detecta e notifica incidentes (ZABBIX, 2023).A arquitetura do Zabbix, demonstrada na Figura 5, é composta por uma interface *web*, pelo servidor Zabbix que atua como repositório central, por sondadores adicionais que coletam dados para o servidor Zabbix denominados Zabbix *Proxies*, e por um banco de dados para armazenamento de configurações relacionadas à sondagem e armazenamento dos dados coletados (ZABBIX, 2023).

Figura 5 - Arquitetura Zabbix.



Fonte: (VACCHE; LEE, 2013).

Para melhor compreensão, é necessário destacar os principais recursos oferecidos pela ferramenta (ZABBIX, 2023):

- Itens: métricas que especificam informações a serem coletadas, método de coleta, intervalo de coleta, período de armazenamento, e pré-processamento;

- *Templates*: Moldes de configuração aplicados aos dispositivos cadastrados, que caracterizam itens, gráficos, *dashboards*, etc. O Zabbix oferece nativamente diversos *templates* para produtos específicos, porém o usuário pode criar seus próprios templates;
- *Dashboards*: Telas que apresentam valores e gráficos dos itens coletados;
- *Triggers*: Alertas de incidentes previamente especificados pelo usuário;
- Descoberta de rede: Recursos para descoberta e cadastro de dispositivos na rede;
- *Low-level discovery*: Recurso para descoberta de itens dinâmicos, como interfaces de rede ativas em um dispositivo. Fornece um meio de coleta através de mensagens SNMP *Get-next*;
- *Zabbix Agent*: Serviço implantado no dispositivo gerenciado para coleta de informações através de chamadas de sistema nativas. Dispositivos com o agente zabbix podem se cadastrar automaticamente no servidor.

LINK LAYER DISCOVERY PROTOCOL (LLDP)

O *Link Layer Discovery Protocol* (LLDP) é um protocolo implementado em dispositivos IEEE 802, sendo especificado pelo padrão IEEE 802.1AB. O LLDP define a troca de mensagens entre dispositivos IEEE 802 com o objetivo de popular a LLDP-MIB, providenciada por um agente SNMP, com informações que ajudem a caracterizar a topologia da rede (CONGDON, 2002).

Periodicamente o agente LLDP, *software* existente em um dispositivo que implementa o protocolo LLDP, envia mensagens contendo informações relevantes a caracterização da topologia sobre o dispositivo através de todas suas interfaces de rede cuja transmissão de mensagens LLDP esteja habilitada. Os dispositivos adjacentes que possuam agente LLDP e agente SNMP então armazenam estas informações na LLDP-MIB durante um período especificado na mensagem LLDP recebida (CONGDON, 2002).

VIRTUAL LOCAL AREA NETWORK (VLAN)

Uma *Virtual Local Area Network* (VLAN) é uma emulação de uma rede local que permite o agrupamento lógico de dispositivos IP conectados a diferentes equipamentos de interconexão. A segmentação da rede em VLANs diminui os domínios de colisão - grupo de dispositivos que dividem uma largura de banda -, além de possibilitar que dispositivos de interconexão atendam dispositivos finais pertencentes a subredes diferentes, ou, que dispositivos de uma mesma subrede conectados à equipamentos de interconexão distintos se comuniquem (OPPENHEIMER, 2011).

Uma VLAN configurada em um dispositivo possui um identificador único. Todas as interfaces de rede de dispositivos com suporte a VLAN possuem um identificador de VLAN associado. As interfaces de rede então podem ser configuradas como (OPPENHEIMER, 2011):

- *Untagged*: As interfaces *untagged* são geralmente utilizadas para a conexão com dispositivos finais que não possuem configurações de VLAN. As interfaces *untagged* aceitam quadros *Ethernet* sem *tag* de VLAN que estejam ingressando no dispositivo. Após o ingresso, é acrescentado ao quadro um *tag* de VLAN contendo o identificador de VLAN associado à interface. A interface *untagged* somente repassa quadros cuja *tag* de VLAN seja a mesma do identificador da VLAN associada a interface.
- *Tagged:* As interfaces *tagged* carregam tráfego de múltiplas VLANs. Interfaces *tagged* não aceitam quadros que não contenham *tag* de VLAN.

METODOLOGIA

A pesquisa e o desenvolvimento levam em consideração as ferramentas que já estavam implementadas e os objetivos previamente estabelecidos pela equipe quanto ao uso dessas ferramentas.

Ao identificar os responsáveis pelas decisões que afetam a infraestrutura de TI, foi necessário questioná-los sobre o tráfego da rede, faixas de endereços IPv4, documentação de rede, etc. Como não havia disponibilidade dos responsáveis pela rede para responder todas estas questões, e a documentação existente não estava atualizada, foi necessário combinar as informações contidas nas ferramentas previamente utilizadas pelo setor, a documentação atual e a aplicação dos conhecimentos próprios para identificar os equipamentos de interconexão, servidores e serviços oferecidos.

Após a caracterização da rede, foram planejadas as soluções a serem implementadas com o acompanhamento dos supervisores. Logo, as soluções foram implementadas e então otimizadas. Os resultados foram apresentados à equipe e foi criada a documentação do projeto.

INFRAESTRUTURA DA TI

A análise da infraestrutura da rede do HUSM é complexa, contando com um elevado número de serviços virtualizados e equipamentos físicos de diferentes fornecedores e modelos. Os serviços oferecidos seguem o regimento estabelecido pela Diretoria de Tecnologia da Informação da EBSERH.

Parte dos serviços oferecidos pelo SETISD-HUSM é dependente da infraestrutura da Universidade Federal de Santa Maria, como acesso à Internet e ao Sistema Integrado de Ensino, e da Rede Nacional de Ensino Pesquisa.

O monitoramento da rede é contemplado pelas ferramentas:

- Zabbix, para construção de gráficos e geração de alertas;
- Cacti, para construção de gráficos e retenção histórica de dados;
- *Ubiquiti UniFi Controller*, para gerência dos *access points* UniFi;

Com a finalidade de documentação, o setor utiliza o gerenciador de projetos *Redmine*.

FERRAMENTAS DE MONITORAMENTO

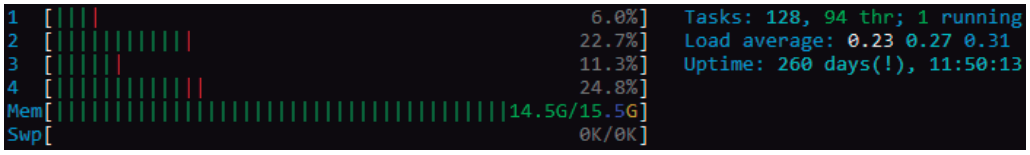
Existiam duas instâncias do Cacti na rede:

- Servidor Cacti 0.8: em processo de desativação, este contava com cadastros de dispositivos gerenciáveis desatualizados, como faixas de endereço IPv4 que não estavam mais em uso e dispositivos que não faziam mais parte da rede. Também, não monitorava dispositivos que haviam sido introduzidos na rede no último ano;
- Servidor Cacti 1.2: o propósito deste era substituir o servidor Cacti desatualizado. Este não possuía nenhum dispositivo cadastrado.

De forma geral, nenhuma instância da ferramenta Cacti estava cumprindo seu propósito. O servidor Zabbix, na Versão 4.2, contava com cadastros de dispositivos gerenciáveis desatualizados, além do uso excessivo de recursos computacionais. Utilizando o utilitário *htop*, uma aplicação para visualização de processos, é possível obter métricas do uso de memória e utilização de CPU referentes à máquina na qual o Zabbix está sendo executado, como demonstrado na Figura 6. O uso excessivo de recursos era resultado de:

- Parâmetros de configuração do banco de dados definidos pelo usuário que carregavam parte do banco de dados para a memória;
- Coleta de itens redundantes e/ou desnecessárias como estatísticas referentes a todas as interfaces de rede de todos os dispositivos gerenciáveis;
- Construção de gráficos desnecessários;
- Intervalos de sondagem desnecessariamente curtos.

Figura 6 - Uso de recursos do servidor Zabbix antigo.



Fonte: Autor.

FERRAMENTAS UTILIZADAS

As ferramentas utilizadas para o desenvolvimento da pesquisa já existiam na infraestrutura de TI do HUSM e faziam parte dos requisitos da gerência.

CACTI

O Cacti já existia na infraestrutura de TI do SETISD-HUSM e fazia parte dos requisitos da gerência. A motivação da gerência quanto ao Cacti era preferência pelos gráficos construídos pelo

Cacti quanto aos gráficos construídos pelo Zabbix. Levando em conta os problemas mencionados neste trabalho, e as características do sistema *RRDTool*, o Cacti é utilizado para retenção de dados por longos períodos de tempo.

ZABBIX

O Zabbix, no contexto do SETISD-HUSM, tem como função principal a geração de alertas e notificações de incidentes. A flexibilidade da ferramenta e seu alto nível de automatização diminuem a necessidade de manutenção constante. As regras de descoberta facilitam a criação e remoção dinâmica/automática de cadastro de elementos de rede, itens de sondagem, gatilhos de incidentes e gráficos. O recurso de dependência de *triggers* permite a rápida identificação da origem do problema, evitando a geração desnecessária de um grande número de incidentes, por exemplo, a sinalização de uma queda de energia.

RESULTADOS

A lógica de monitoramento foi remodelada a fim de evitar redundâncias com as demais ferramentas e desperdícios de recursos computacionais.

Tanto para o Cacti como para o Zabbix foram criados *templates* para os diferentes dispositivos, levando em conta modelo e fabricante. Utilizando os *templates* junto aos recursos de descoberta de rede, a necessidade de configurações relacionadas ao monitoramento de novos dispositivos foi minimizada.

O Cacti agora serve ao propósito de construção de gráficos e retenção histórica de estatísticas, para possibilitar a identificação de padrões e eventos sazonais.

O Zabbix atende as necessidades da Gerência de Falhas e da Gerência de Desempenho gerando alertas para incidentes de falha e indicativos de eventuais falhas. Foi abandonada a retenção de estatísticas por longos períodos de tempo, armazenando dados por no máximo um mês. A construção de gráficos serve apenas para melhor compreensão dos incidentes. A partir da análise dos problemas no ecossistema de monitoramento, e considerando que o Cacti é um requisito da gerência, a retenção de dados históricos é contemplada pelo Cacti.

O Zabbix monitora todos os dispositivos e serviços da infraestrutura de TI do HUSM, exceto os dispositivos finais como computadores de uso pessoal. Diversas configurações de coleta de dados que antes eram feitas de forma estática agora ocorrem de maneira dinâmica, utilizando os recursos de descoberta de rede e *Low-level Discovery.*

A detecção de incidentes agora leva em conta questões de dependência. Por exemplo, se foi gerado o alerta referente à bateria de um *NoBreak* estar esgotada, não há necessidade da geração de alertas referentes à indisponibilidade.

A pesquisa do presente trabalho foi desenvolvida na busca de informações sobre a infraestrutura. Documentações referentes à interconexões entre *switches*, rotas, redundâncias e VLANs constavam na ferramenta *Redmine*, cujo acesso era restrito. Para buscar essas informações era necessário consultar diretamente os funcionários, o que dependia da disponibilidade destes, e consultar as ferramentas de monitoramento, que estavam desatualizadas. Mesmo consultando a ferramenta Redmine, ainda não era possível a obtenção completa de informações referentes a todos os serviços e dispositivos, visto que nem todas as alterações e implantações foram documentadas adequadamente. Este problema na documentação impossibilitou a identificação da totalidade dos servidores e serviços oferecidos pelo SETISD-HUSM ao cliente interno. Dadas as limitações de tempo, e na documentação existente, não foi possível contemplar o monitoramento mais específico de servidores com base nos serviços oferecidos.

Para noções básicas de topologia foi necessário desenvolver uma ferramenta para fazer buscas na LLDP-MIB dos *switches* para se ter uma visão básica da topologia da rede e na MIB dot1dBridge para informações referentes a VLANs e redundâncias. Mesmo assim ainda não foi possível ter uma visão completa da topologia, já que alguns dispositivos, mesmo tendo o agente LLDP habilitado, não possuíam permissão de leitura para a LLDP-MIB.

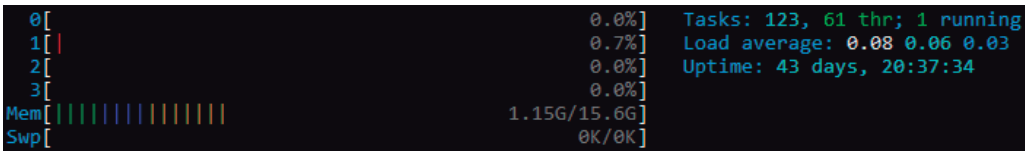
As atividades envolvendo o Zabbix eram inicialmente voltadas a atualização da versão 4.2 para a versão 6.0. A atualização não foi realizada: os requisitos mínimos de *softwares* dos quais o Zabbix depende não foram atingidos. O sistema operacional instalado no dispositivo no qual o Zabbix estava instalado estava desatualizado e sem suporte. A atualização do sistema operacional encontrou diversos problemas referentes a repositórios. A migração do banco de dados do servidor Zabbix para outra máquina, com sistema operacional e versão do Zabbix ambos atualizados, não foi possível devido a incompatibilidade entre banco de dados e a versão 6.0 do Zabbix.

Não havia monitoramento sendo realizado pelo Cacti novo, uma vez que este recém estava sendo implantado. O cadastro de dispositivos que antes acontecia de forma manual, foi pensado para acontecer de forma automática, levando em conta a faixa de endereço IPv4, modelo e fornecedor.

A coleta de dados era baseada em *templates* encontrados na Internet e templates padrões do Cacti. Agora, templates foram criados para cada tipo de dispositivo, levando em conta os objetivos de monitoramento quanto ao uso do Cacti, e a dinamicidade dos objetos gerenciáveis dos dispositivos.

Utilizando novamente o utilitário *htop*, foi possível observar que o servidor Zabbix agora utiliza em média 8% da memória disponível (Figura 7), enquanto o servidor Zabbix antigo consumia em média 93% (Figura 6).

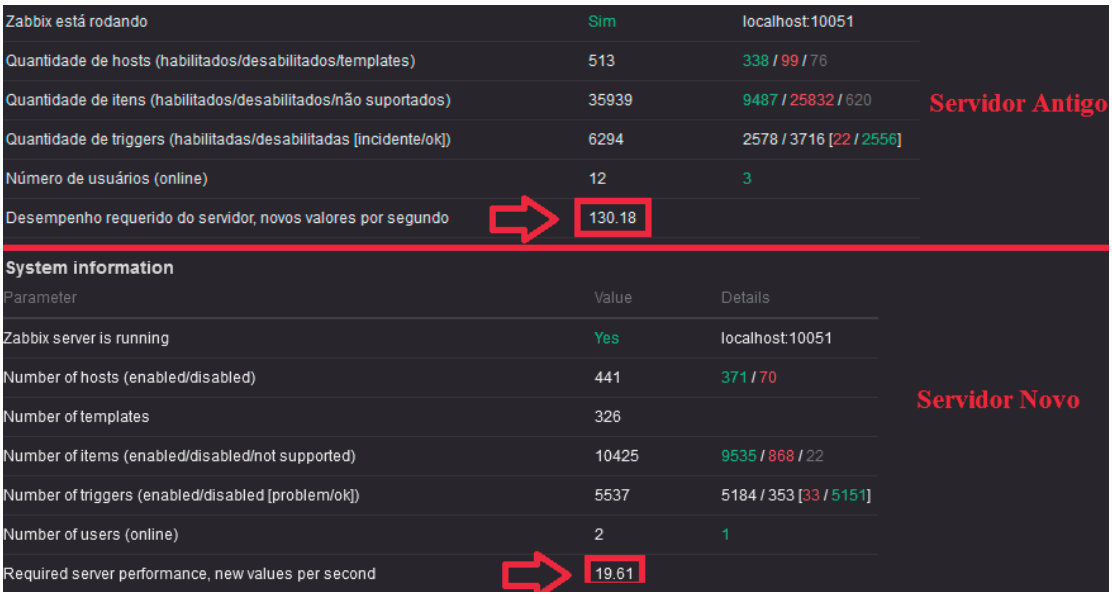
Figura 7 - Uso de recursos do servidor Zabbix novo.



Fonte: Autor.

O servidor Zabbix antigo recebia em média 130 valores por segundo, enquanto o servidor novo recebia em média 20 valores por segundo (Figura 8).

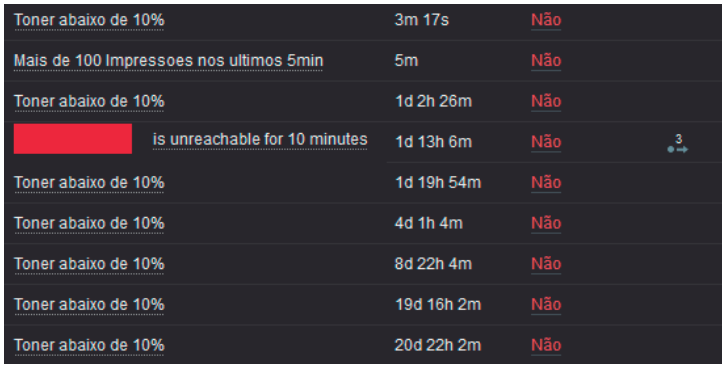
Figura 8 - Comparação entre valores por segundo.



Fonte: Autor.

A Figura 9 e a Figura 10 mostram a comparação entre a notificação de incidentes do servidor Zabbix antigo e do servidor Zabbix novo. Em determinado momento o servidor Zabbix antigo notificou apenas incidentes relacionados ao nível de tinta em *toners* de impressoras e um incidente relacionado à indisponibilidade. Neste mesmo momento, o servidor novo notificou incidentes relacionados à performance e indisponibilidade.

Figura 9 - Incidentes notificados pelo servidor antigo.



Fonte: Autor.

Figura 10 - Incidentes notificados pelo servidor novo.

Fonte: Autor.

Para auxiliar na análise dos valores recebidos para os dispositivos da rede, foram criadas telas para sumarizar as informações referentes à performance de um determinado dispositivo.

A Figura 11 demonstra um exemplo de tela para um *acess point*, contendo informações sobre disponibilidade e métricas de performance relacionadas a dispositivos conectados, uso de memória e tráfego em cada interface.

Figura 11 - Tela para *access point*.

Fonte: Autor.

Para otimizar a automatização das ferramentas de monitoramento, ou seja, diminuir a necessidade dos administradores da rede de realizar configurações a cada alteração na infraestrutura de TI. De certa forma este objetivo foi atingido: cadastros de dispositivos e as configurações referentes ao monitoramento de interfaces, sensores de temperatura, espaço em disco entre outros são realizados de forma automática pelo Zabbix.

Porém, dados que envolvem VLANs, alterações de topologia, e enlaces de redundância não foram possíveis de se obter de forma automatizada. Isso se dá ao fato de que as consultas feitas utilizando o protocolo SNMP às MIBs referentes a estas informações envolverem índices diferentes nas MIBs para uma mesma interface. A automatização destas informações envolveria a utilização de *scripts* para consultas SNMP e manipulação de dados.

Segundo Zabbix (2023), a execução de *scripts* necessita iniciar um processo filho pelo servidor Zabbix, resultando em uso excessivo de recursos computacionais. Também, a complexidade de tais *scripts* tornaria difícil a compreensão de funcionários que eventualmente venham a utilizar a ferramenta. Tendo em vista que alterações na rede referentes a VLANs, redundâncias e topologia de *switches*, não é comum no contexto do SETISD-HUSM, estas configurações são feitas manualmente pelos administradores da rede.

CONCLUSÃO

A importância de soluções de monitoramento de redes de computadores foi observada durante a execução da pesquisa: a sondagem referente à saúde da rede e seus serviços permite aos gerentes da rede trabalhar de forma proativa. A aplicação dos conhecimentos construídos ao longo da graduação permitiu a implementação de soluções de monitoramento que atendessem aos objetivos da gerência de forma eficiente.

Analisando as soluções de monitoramento existentes no setor, foi possível identificar problemas referentes ao uso de recursos computacionais e à implementação de uma lógica de monitoramento ineficiente. Tendo isto em consideração, o objetivo proposto do trabalho foi alcançado com sucesso, promovendo um melhor e mais eficiente monitoramento da infraestrutura de rede. A execução deste trabalho tinha como principal objetivo otimizar a automatização das ferramentas de monitoramento, ou seja, diminuir a necessidade dos administradores da rede de realizar configurações a cada alteração na infraestrutura de TI, como por exemplo: cadastros de dispositivos e as configurações referentes ao monitoramento de interfaces, sensores de temperatura, espaço em disco entre outros são realizados de forma automática pelo Zabbix.

Porém, dados que envolvem VLANs, alterações de topologia, e enlaces de redundância não foram possíveis de se obter de forma automatizada. Isso se dá ao fato de que as consultas feitas utilizando o protocolo SNMP às MIBs referentes a estas informações envolverem índices diferentes nas MIBs para uma mesma interface. A automatização destas informações envolveria a utilização de *scripts* para consultas SNMP e manipulação de dados.

Segundo Zabbix (2023), a execução de *scripts* necessita iniciar um processo filho pelo servidor Zabbix, resultando em uso excessivo de recursos computacionais. Também, a complexidade de tais *scripts* tornaria difícil a compreensão de funcionários que eventualmente venham a utilizar a

ferramenta. Tendo em vista que alterações na rede referentes a VLANs, redundâncias e topologia de *switches*, não é comum no contexto do SETISD-HUSM, estas configurações são feitas manualmente pelos administradores da rede.

Levando em conta cada tipo de dispositivo gerenciável e seu papel na rede, foi possível implementar soluções de monitoramento mais eficientes nas dimensões de falha, contabilidade e desempenho referentes ao modelo FCAPS foram contempladas utilizando as ferramentas Cacti e Zabbix.

No decorrer do artigo foi relatado o problema com a atualização do servidor Zabbix. A partir deste fato, recomenda-se que um servidor de teste seja implantado e periodicamente sincronizado com o servidor Zabbix de produção. O servidor de teste deve ter seu sistema operacional e versão do Zabbix atualizados antes do servidor de produção para testes de compatibilidade e estabilidade.

A monitorização dos servidores com base nos serviços disponibilizados não pôde ser abrangida. Devido às restrições temporais e à documentação existente, não foi viável incluir a monitorização mais específica de servidores em função dos serviços prestados. A importância de uma documentação compreensível e completa é enfatizada por diversos autores:

- Para Gregory (2008), Manzuik, Gold e Gatford (2007) e Maiwald e Sieglein (2002) planejamentos de segurança e recuperação de desastres dependem fortemente de uma documentação completa e atualizada da infraestrutura;
- Para Smith (2007), as ações de execução, manutenção e melhorias de um sistema dependem do quanto o administrador conhece este sistema;
- Para Oppenheimer (2011), a documentação da infraestrutura de TI é um dos meios que um novo funcionário ou analista externo possui para compreensão da rede. A documentação ajuda a tomada de decisões referentes à implantação de novos serviços ou alteração na infraestrutura de TI.

Recomenda-se que estudos subsequentes enfoquem a implementação de um sistema de documentação e um inventário, além de propor uma abordagem para a análise e o tratamento de registros de eventos.

REFERÊNCIAS

BERRY, Ian *et al.* ***The Cacti Manual***. Disponível em https://files.cacti.net/docs/html/. Acesso em: 03 nov. 2022.

BOGAERDT,Alex. **Rrdtutorial.** Disponível em https://oss.oetiker.ch/rrdtool/tut/. Acesso em: 10 dez. 2022.

CACTI. ***What is Cacti?*** Disponível em https://www.cacti.net/info/cacti. Acesso em: 13 out. 2023.

CHUNJIN, Zhang; SHUJUAN, Ji. ***A SNMP-base broadcast storm identification method in VLAN.*** Disponível em https://www.researchgate.net/publication/266646385_A_SNMP-base_broadcast_storm_identification_method_in_VLAN>. Acesso em: 15 mar. 2023.

CONGDON, Paul. ***Link Layer Discovery Protocol and MIB v0.0.*** Disponível em https://www.ieee802.org/1/files/public/docs2002/lldp-protocol-00.pdf. Acesso em: 14 mar. 2013.

CLEMM, Alexander. ***Network Management Fundamentals***. 1. ed. Indianápolis, Indiana: Cisco Press, 2006.

EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES. **Setor de Tecnologia da Informação e Saúde Digital**. Disponível em: https://www.gov.br/ebserh/pt-br/hospitais-universitarios/regiao-sul/husm-ufsm/governanca/superintendencia/setor-de-tecnologia-da-informacao-e-saude-digital/STISD. Acesso em: 15 dez. 2022.

GREGORY, Peter. ***IT Disaster Recovery Planning For Dummies***. 1. ed. Indianápolis, Indiana: Wiley Publishing, Inc., 2008.

KUROSE, James; ROSS, Keith. ***Computer Networking: A Top-Down Approach***. 6. ed. Estados Unidos: Pearson, 2012.

MAIWALD, Eric; SIEGLEIN, William. ***Security Planning & Disaster Recovery***. 1. ed. Berkeley, Califórnia: McGraw-Hill Osborne Media, 2002.

MANZUIK, Steven; GOLD, Andre; GATFORD, Chris. ***Network Security Assessment:*** *From Vulnerability to Patch*. 1. ed. Rockland, Massachusetts: Syngress, 2006.

MAURO, Douglas; SCHMIDT, Kevin. ***Essential*** **SNMP**. 1. ed. Sebastopol, Califórnia: O'Reilly Media, 2001.

MCCLOGHRIE, Keith; ROSE, Marshall. ***Management Information Base for Network Management of TCP/IP-based internets*** **- MIB-II, STD 17. RFC 1213**. 1991.

OPPENHEIMER, Priscilla. ***Top-Down Network Design***. 3. ed. Indianápolis, Indiana: Cisco Press, 2010.

PHALTANKAR, Kaustubh. ***Practical Guide for Implementing Secure Intranets and Extranets***. 1. ed. Norwood, Massachusetts: Artech House Publishers, 1999.

SMITH, Roderick. ***Linux Administrator Street Smarts:*** *A Real World Guide to Linux Certification Skills*. 1. ed. Indianápolis, Indiana: *Wiley Publishing*, Inc., 2007.

VACCHE, Andrea; LEE, Stefano. ***Mastering Zabbix***. 1. ed. *Birmingham*, Reino Unido: *Packt Publishing*, 2013.

ZABBIX. **Zabbix Manual**. Disponível em https://www.zabbix.com/documentation/6.0/en/manual. Acesso em: 10 jan. 2023.