Implantação do Zabbix na UFAL Campus Arapiraca

José Junio da S. Calú[1], Felipe da S. Leite[1], Rômulo N. de Oliveira [1], Cárlisson B. T. Galdino[1]

[1]Núcleo de Tecnologia da Informação – Universidade Federal de Alagoas (UFAL)
CEP – 57309-005 – Arapiraca – AL – Brasil

{junio.calu,felipe.leite}@arapiraca.ufal.br
{romulo,carlisson}@nti.ufal.br

Abstract. *Managing a network efficiently, using appropriate tools is essential to ensure the good quality of the services offered. From this, it becomes possible to avoid problems such as deterioration of equipment, underutilization of bandwidth, or even delays for solving incidents. In this sense, this article seeks to demonstrate how the Zabbix tool can assist in the management of a network infrastructure, taking as its case study its implementation in a federal institution of higher education. The solution is low-cost and has shown promise, offering relevant data and reports to management, enabling preventive actions to be carried out on the various assets of the network.*

Resumo. *Administrar uma rede de maneira eficiente, utilizando de ferramentas adequadas é fundamental para garantir a boa qualidade dos serviços oferecidos. A partir disso, passa a ser possível evitar problemas como deterioração de equipamentos, subutilização de banda, ou mesmo atrasos para solução de incidentes. Nesse sentido, este artigo busca demonstrar como a ferramenta Zabbix pode auxiliar na gerência de uma infraestrutura de rede, tomando como estudo de caso a sua implantação em uma instituição federal de ensino superior. A solução é de baixo custo e se apresentou promissora, oferecendo dados e relatórios relevantes para a administração, possibilitando a realização de ações preventivas nos diversos ativos da rede.*

1. Introdução

Durante o primeiro estágio do que seria a Internet, nos anos 60, e nas duas décadas seguintes, a necessidade de se estabelecer uma política de gerenciamento de rede era praticamente inexistente [Stevenson 1995]. As primeiras redes de computadores interconectavam apenas universidades para fins de pesquisa. Mesmo na década de 70, com o uso do computador se expandindo para outras áreas além da pesquisa acadêmica, e com mainframes sendo utilizados no processamento de dados por parte de empresas e governos, a demanda por um gerenciamento de rede ainda não era prioridade. No mainframe o administrador tinha o controle total de tudo que se passava dentro da empresa. Em um único sistema ou computador o administrador tinha formas de monitorar de perto o espaço em disco, CPU disponível, número de utilizadores presentes, tempo de resposta das transações, etc, que é uma realidade bem diferente da atual [Leiner et al. 2009, Kurose et al. 2013, p. 555].

Com a difusão dos computadores pessoais, também tivemos que lidar com o gerenciamento de diversos recursos, como por exemplo: tráfego de dados, integridade de informação, banco de dados, sistemas distribuídos, etc. Houve também a possibilidade do uso de computadores em locais mais afastados do "data center", onde antes o antigo mainframe limitava a distância do terminal. As instituições passaram a ter conjuntos de ilhas de computadores, isolados uns dos outros, não necessariamente próximos aos servidores de rede [Cisco Systems 2004, p. 132]. Essa expansão da rede interna institucional trouxe alguns problemas: administração dos sistemas e usuários, a segurança da informação, e o monitoramento da disponibilidade e do comportamento dos serviços oferecidos. No contexto de redes de computadores, com o aumento da banda de tráfego e a forte dependência da rede para os sistemas integrados e sistemas web, cada vez mais se tornava evidente a necessidade de uma solução para o gerenciamento eficiente e com baixo *overhead* [Ford et al. 1999, p. 45].

O objetivo das tecnologias de gerenciamento de rede é reduzir os riscos e garantir segurança e disponibilidade, requisitos essenciais para os sistemas corporativos [Yemini 1993, p. 1]. Nesse sentido, a Universidade Federal de Alagoas (UFAL), Campus Arapiraca, possui centenas de ativos de rede. Isso acaba resultando em uma quantidade exorbitante de variáveis a serem analisadas durante o processo de resolução de um problema na rede. Diante da complexidade, esses problemas podem até mesmo passar despercebidos aos olhos do gerente de rede, seja pela falta de uma visão panorâmica do quadro, ou de dados precisos para se traçar um diagnóstico das causas de um incidente. E foi isso que se constatou, tão logo posto em estado de produção o Zabbix [Zabbix 2020]. Vieram à tona desde de problemas menos graves como servidores virtuais "reclamando" de insuficiência de memória RAM, até problemas mais graves como a identificação de deterioração a nível de hardware em dispositivos custosos do ponto vista financeiro à instituição.

Dada a importância do gerenciamento de rede, e após uma breve contextualização histórica de como se deu a evolução das redes de computadores até os dias atuais, este trabalho traz como contribuição um estudo de caso sobre a implantação da ferramenta de monitoramento Zabbix na UFAL, Campus Arapiraca.

2. Zabbix

O Zabbix é uma plataforma de gerenciamento de rede desenvolvida por Alexei Vladishev em meados do ano 2000 e agora mantida pela Zabbix LLC [Zabbix 2020]. O Zabbix suporta tanto o *trapping* (coleta passiva de dados) SNMP (Simple Network Management Protocol) quanto o *polling* (coleta ativa). Possui ainda suporte aos protocolos: IPMI, JMX, Monitoramento VMware, ICMP Ping e SSH. Traz a possibilidade de monitoramento individual de Portas TCP. Tem um agente próprio para instalação em dispositivos que não deem suporte ao SNMP, podendo ser configurado para funcionar em modo ativo ou modo passivo. Seu Web *Frontend* provê recursos para autenticação de usuaŕios, visualização e criação de gráficos, mapas, alertas de incidentes, entre outros.

A comunidade do Zabbix é ativa, onde se compartilham, *templates*, modelos de monitoramento prontos contendo itens de coleta, gráficos e configurações de alerta aplicáveis à dispositivos ou elementos já conhecidos pela comunidade [Benicio 2015, p. 41]. A ferramenta também fornece uma API para atualizações em massa e integração com ferramentas de terceiros. As notificações de incidentes podem ser visualizadas no Web *Frontend* ou configuradas para serem recebidas por email, SMS, Jabber, Ez Texting ou scripts de alertas customizáveis.

Para instalação do Zabbix, a Zabbix LLC mantém um repositório para as distribuições GNU/Linux mais populares, como Ubuntu, Debian e Fedora, com pacotes pré-compilados da ferramenta em sua versão mais recente e estável. Configurado o repositório, o procedimento se resume a utilizar o gerenciador de pacotes da distribuição para baixar as dependências compatíveis com o SGBD suportado pelo Zabbix (MySQL, Oracle, PostgreSQL, SQLite ou IBM DB2), criar um banco de dados, instalar o Apache, habilitar o servidor Zabbix no gerenciador de serviços de inicialização do sistema (SysVinit, SystemD ou Upstart) e concluir o procedimento fornecendo alguns informações adicionais no Web *Frontend*.

2.1. Zabbix e SNMP

O SNMP [Case et al. 1990] é um dos principais protocolos usados pelo Zabbix para coleta de métricas de monitoramento de dispositivos. Criado em 1990 e descrito no RFC 1157, por se tratar de um protocolo aberto, rapidamente se tornou padrão de monitoramento na Internet, com os fabricantes de dispositivos de rede o embutindo já na produção em fábrica [Stevenson 1995].

O monitoramento SNMP depende de uma análise do MIB (Management information base) para identificar recursos monitoráveis de um dispositivo, como por exemplo: estatísticas de tráfego de rede de uma interface *ethernet*, estados de operação dessa mesma interface (Up ou Down), logs de sistema, etc. Existem MIBs do tipo aberto (definidos em RFCs) e os proprietários criados pelos fabricantes de dispositivos. Um MIB nada mais é do que um banco de dados formado por uma coleção de objetos gerenciáveis dispostos em formato de árvore. Os arquivos contidos no banco de dados MIB são arquivos de texto plano, geralmente nomeados com a extensão ".mib". Cada objeto gerenciável é descrito nesses arquivos segundo a notação ASN.1 e contém um identificador de objetos (OID), um tipo, uma faixa de valores possíveis, seu relacionamento com outros objetos, o tipo de operação aceita pelo objeto (requisições SNMP Get ou Set), podendo também conter uma breve descrição textual sobre sua utilidade [Kurose et al. 2013, 566].

Para facilitar a tarefa de análise de um MIB e o entendimento de cada OID contido nele, foram criados os MIB *Browsers*, ferramentas utilizadas para "navegar" pela árvore MIB. A maioria dos MIB *Browsers* possuem um recurso integrado para enviar requisições Gets ou Sets SNMP [Extreme Networks 2020].

2.2. Zabbix e Agentes Zabbix

Na ausência de um agente SNMP nativo no dispositivo alvo do monitoramento, o Zabbix disponibilizada agentes próprios como alternativa. O servidor Zabbix se comunica com esses agentes na porta TCP 10050 por meio de um protocolo próprio de troca de informações em formato JSON, onde as métricas de monitoramento coletadas são extraídas diretamente das diretivas do sistema operacional onde o agente é instalado.

Para se poder monitorar usando o Agente Zabbix, três etapas são necessárias: cadastro manual do host no Web *Frontend*, associação do *template* de monitoramento compatível com o sistema operacional, e instalação do agente através do repositório da Zabbix LLC. Esse procedimento pode ser resumido a uma ou duas etapas, configurando os agentes logo na instalação para trabalharem no modo ativo de monitoramento. No modo ativo os agentes se auto registram no Servidor Zabbix, bastando que o administrador defina o IP do servidor no parâmetro "ServerActive" do seu arquivo de configuração.

3. Métodos

A abordagem de implantação da plataforma, adotada pela equipe de TI da instituição pode ser resumida em três fases: pesquisa de mercado, instalação do servidor Zabbix, e reuniões em equipe para elicitação dos elementos de rede a serem monitorados. Como pode ser visto com mais detalhes na Figura 1.

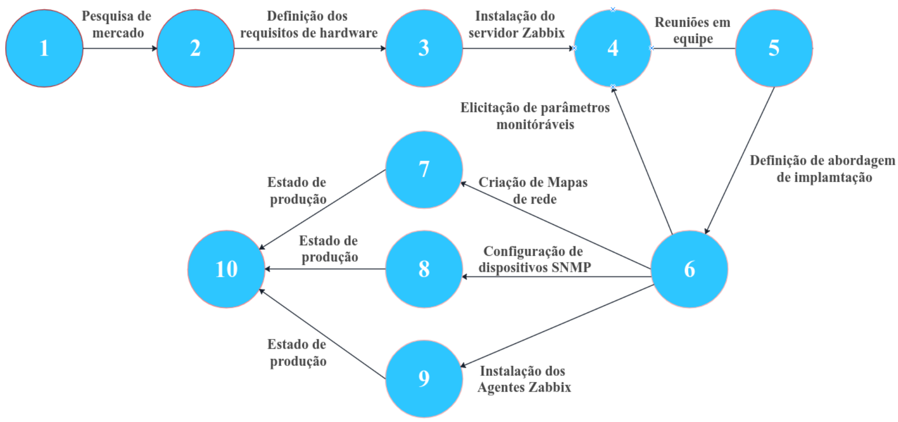

Figura 1. Gráfico PERT do fluxo de trabalho de implantação do Zabbix [Autor 2020]

Na primeira fase buscou-se respaldo na literatura já existente, onde comparativos entre plataformas de gerenciamento como [Kovacs 2016], [dos Santos and Martins 2016] e [Black 2008] podem ser encontrados. Black (2008) compara oito ferramentas de gerenciamento, e sintetiza em uma tabela os prós e contras de cada uma (Tabela 1). A ferramenta Nagios, apesar de parecer completa, possui limitações como o suporte não *standard* ao SNMP e Autodiscovery, disponibilizados como plugins mantidos pela comunidade, e uma interface mais simples também fornecida opcionalmente. Com uma ressalva para o software Spiceworks, que apresenta todas as funcionalidades, exceto o suporte gráfico integral, Black (2008) é categórico ao afirmar que o Zabbix promete ser a ferramenta mais completa dentre as GPL (GNU General Public License), pois une todas as opções que as demais, debaixo de uma interface robusta e amigável.

Uma vez definida a plataforma de gerenciamento, foi dado início ao processo de instalação da aplicação. Os requisitos mínimos de hardware são 128MB de memória RAM, 256MB de armazenamento livre em disco. Entretanto, o consumo de memória e CPU aumentam a depender da quantidade de hosts a serem monitorados, e se o gerente almeja manter um longo histórico dos parâmetros de rede coletados, *gigabytes* de espaço em disco deverão ser reservados. Num cenário com mais de mil hosts, por exemplo, a demanda por memória sobe para 8GB, acompanhada de uma CPU de 8 núcleos [Zabbix 2020]. No caso da UFAL, o Zabbix foi instalado em uma máquina virtual com as configurações da Tabela 2.

Finalizada a instalação, deu-se início ao processo de elicitação das métricas a serem coletadas, definidas em reuniões em equipe. Durante as quais definiu-se a seguinte

Tabela 1. Comparação de ferramentas de gerenciamento de redes [Black 2008]

	Cacti	Nágios	ZenOSS	OpManager	BigBrother4	Spiceworks	Look@LAN	Zabbix
SLA Reports	Não	Através de Plugin	Não	Em desenvolvimento	Sim	Sim	Não	Sim
Auto Discovery	Através de plugin	Através de Plugin	Sim	Sim	Sim	Sim	Sim	Sim
Agente	Não	Sim	Não	Não	Sim	Sim	Não	Sim
SNMP	Sim	Através de Plugin	Sim	Sim	Sim	Sim	Sim	Sim
Syslog	Não	Através de Plugin	Sim	Sim	Sim	Sim	Não	Sim
Permite scripts externos	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim
Plugins	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Linguagem que foi escrito	PHP	Perl	Python e Zope	Perl e Python	C	Ruby	C	C e PHP
Gatilhos/alertas	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Front-end web	Controle Completo	Controle Parcial	Controle Completo	Controle Completo	Controle Completo	Controle Completo	Não	Controle Completo
Monitoramento distribuído	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Inventário	Através de Plugin	Através de Plugin	Sim	Sim	Sim	Sim	Não	Sim
Método de armazenamento de dados	RRDTool. MySQL. PostgreSQL em desenvolvimento	MySQL. MS-SQL.	RRDTool para dados de performance. MySQL para eventos	MySQL e MSSQL	Oracle. MSSQL. MySQL	MySQL e SQLite	Não	Oracle. MySQL. PostgreSQL e SQLite
Licenciamento	GPL	GLP	Core: GPL- Pro: ComercialEnterprise: Comercial	Comercial. 30 dias para testar o produto	Comercial	GPL	Freeware	GPL
Geração de gráficos/mapas	Sim/Através de plugin	Sim/Sim	Sim/Sim	Sim/Não	Sim/Sim	Sim/Parcial	Sim/Sim	Sim/Sim
Eventos	Através de plugin	Sim	Sim	Não	Sim	Sim	Não	Sim

Tabela 2. Configurações do servidor virtual com Zabbix Server [Autor 2020]

Configurações de Hardware	
Sistema Operacional GNU/Linux	Debian 10 (Buster) 64 bits
Memória RAM	8 GB
Disco Rígido	60 GB (SATA)
4 Processadores	Common KVM processor 2000 MHz
2 Placas de Rede	Intel 82540EM (Placa em modo bridge)

abordagem: instalação dos Agentes Zabbix nos servidores físicos e virtuais; estudo e testes do SNMP em dispositivos com suporte nativo ao protocolo; mapeamento da rede através do recurso de criação de mapas do Web *Frontend* do Zabbix.

Aos Agentes Zabbix podem ser associados *templates* padrão, fornecidos pela própria ferramenta, embora esses modelos sejam genéricos e inadequados para utilização em ambientes de produção, sendo recomendado ao gerente de rede criar seus próprios *templates* de acordo com as especificidades do ambiente no qual está trabalhando.

A fase de testes dos dispositivos SNMP, foi realizada com auxílio do *MIB browser Ireasoning* [iReasoning 2020]. Essa ferramenta possibilitou encontrar os OIDs corretos para feitura do *template* destinado aos comutadores e *Access Points* da instituição. Para isso, o procedimento foi, baixar do site do fabricante o MIB proprietário do dispositivo em foco, importá-lo por meio da opção gráfica “Load MIBs” da ferramenta, e buscar (opção “Find in MIB tree”) por palavras-chave que faziam referência ao parâmetro a ser monitorado. Por exemplo, para encontrar o OID responsável por fornecer as estatísticas de utilização de CPU de um dado modelo de comutador de camada de enlace, pesquisou-se pela palavra-chave "cpu" que retornou o OID ".1.3.6.1.4.1.1916.1.32.1.2.0" já traduzido para sua forma textual "extremeCpuMonitorTotalUtilization", como observado na Figura 2.

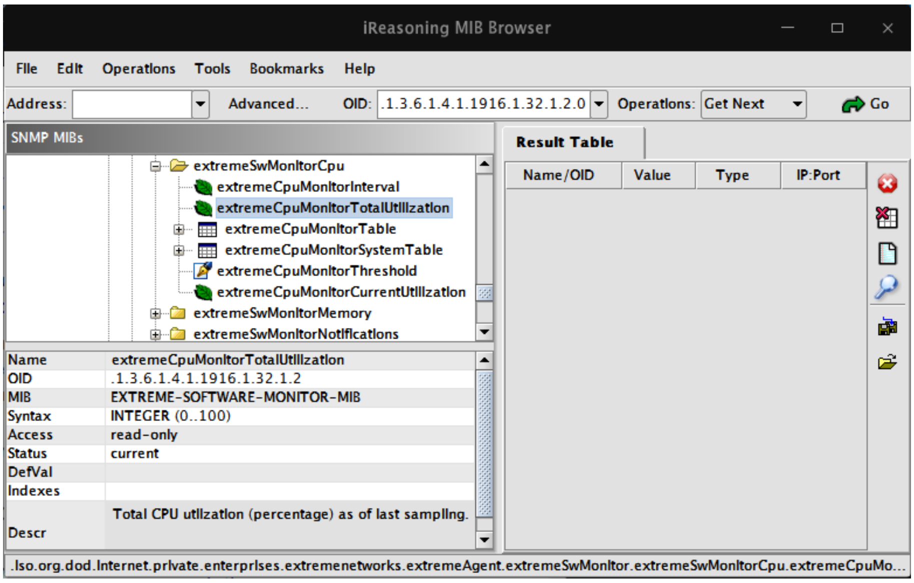

Figura 2. Retorno de uma pesquisa de OID no MIB browser [Autor 2020]

Dessa análise foi possível extrair três dados essenciais para criação de um item de monitoramento de CPU: o tipo da informação INTEGER (um número inteiro no intervalo de 0 a 100), STATUS "current" (indicando que a definição do OID é atual e não obsoleta) e Descr (descrição textual da atribuição do objeto), traduzida como "Utilização total da CPU (porcentagem) desde a última amostragem", indicando que a informação pretendida foi encontrada.

Um item SNMP deve ter obrigatoriamente preenchidos os campos de Nome, Tipo, Chave, SNMP OID, Tipo de informação e Intervalo de atualização, como pode ser visto na Figura 3.

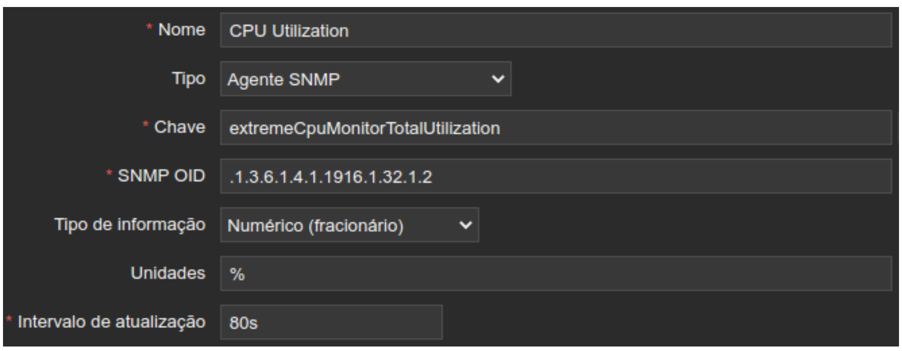

Figura 3. Principais campos para criação de um item SNMP [Autor 2020]

O Zabbix possibilita a aplicação de fatores de conversão sobre os dados recebidos de uma consulta SNMP, ao se especificar, durante a criação do item a unidade de medida (campo "Unidade") pretendida. O OID ifOutOctets que fornece o total de bytes enviados por uma interface de rede, por exemplo, é mais interessante de ser visualizado se convertido para Mpbs ou Gbps.

Após o encerramento dos procedimentos para viabilizar a coleta de métricas de monitoramento dos ativos de rede da instituição, pôde-se dar início ao mapeamento da topologia da rede, através do recurso de criação de mapas do Zabbix.

4. Resultados

A Figura 4 representa a topologia de rede da UFAL. Os ícones circundados por cores representam alertas, disparados por triggers (Figura 5). As cores variam de cinza (incidentes de menor gravidade) a vermelho (maior gravidade).

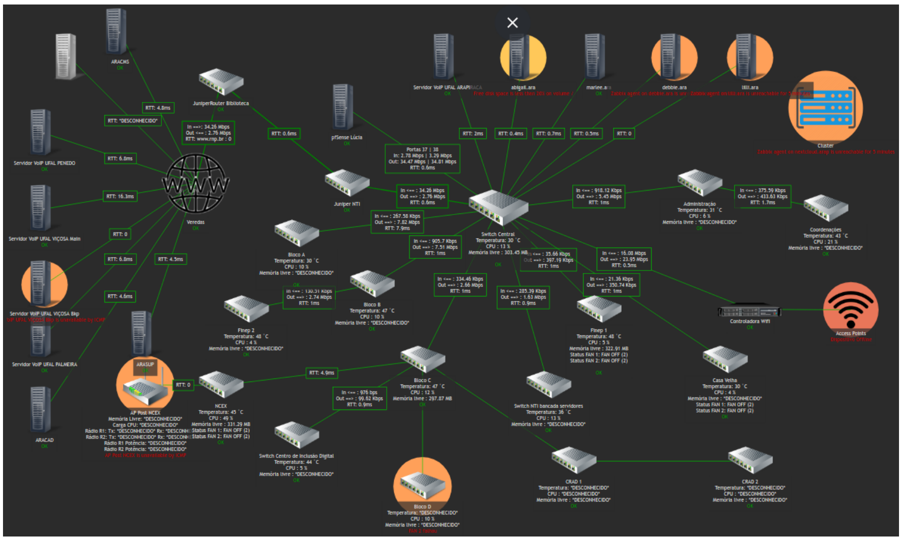

Figura 4. Topologia de rede da UFAL Campus Arapiraca [Autor 2020]

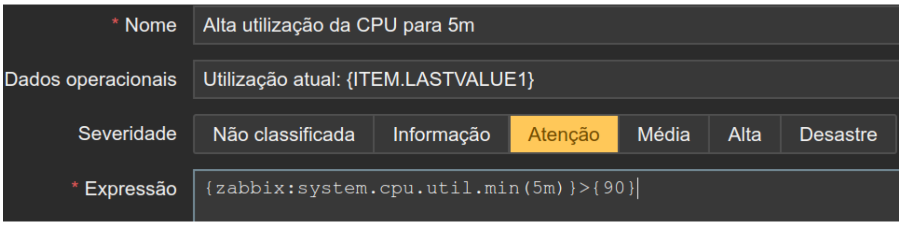

Figura 5. Trigger de CPU [Autor 2020]

As triggers são expressões lógicas que permitem analisar os dados coletados pelos itens, definindo limites saudáveis de operação para um determinado elemento monitorado [Zabbix 2020]. Na Figura 5, a expressão "{zabbix:system.cpu.util.min(5m)}>{90}" analisa os dados de utilização de CPU coletados através do item de nome (chave) "system.cpu.util" do host "zabbix" nos últimos 5 minutos, com a função "min(5)", e verifica se esses valores superam 90% nesse intervalo, com o operador ">{90}", mudando o estado da trigger de "OK" para "INCIDENTE" em caso afirmativo.

A distribuição geográfica dos pontos de acesso sem fio da instituição pode ser visualizada no mapa da Figura 6, que tem como plano de fundo a planta baixa da universidade. Os ícones em vermelho representam *Access Points offline*. Estatísticas de utilização em tempo real de memória, processamento e número de clientes conectados aos dispositivos podem ser visualizadas como descrição textual abaixo dos ícones.

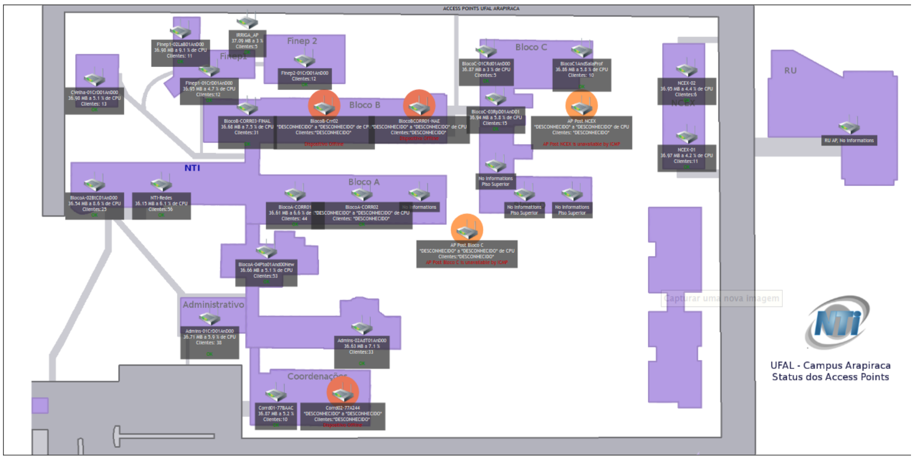

Figura 6. Mapeamento dos Access Points do Campus [Autor 2020]

A distribuição dos servidores da universidade é exibida na Figura 7. Onde cada agrupamento (quadrado) representa uma categoria de serviços. Servidores de armazenamento e compartilhamento de arquivos estão agrupados na categoria "arquivos", por exemplo.

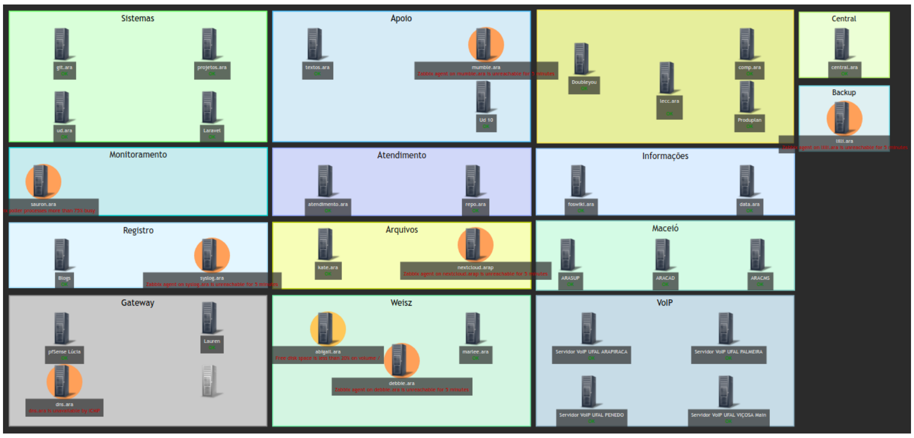

Figura 7. Servidores organizados por categoria [Autor 2020]

Dados de temperatura de um dispositivo de rede, coletados durante um intervalo de 4 meses e 21 dias podem ser visualizados na Figura 8. Picos de temperatura próximos aos 50 graus celsius foram detectados, indicando sobreaquecimento do mesmo. Como medida preventiva, foi construído um anteparo para resfriar o *rack outdoor* exposto ao sol, que comportava o equipamento.

O gráfico exibido na Figura 9, de 3 meses e 13 dias indica oscilações na qualidade do serviço entregue pelo provedor do link de internet da instituição. Analisada essa métrica, relatórios direcionados ao provedor puderam ser elaborados para que o mesmo melhorasse o serviço fornecido.

O consumo de largura de banda da UFAL durante o período de 3 meses e 21 dias (Figura 10), foi base de discussão sobre a necessidade de aumento da capacidade do link.

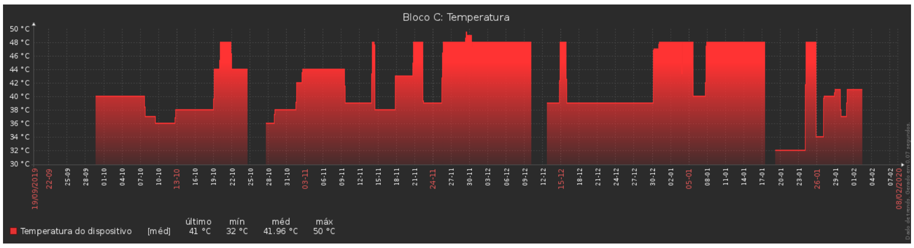

Figura 8. Gráfico de temperatura de um dispositivo de rede [Autor 2020]

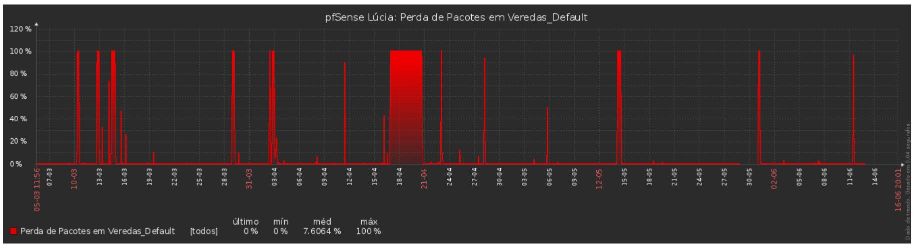

Figura 9. Gráfico de perda de pacotes do link principal da instituição [Autor 2020]

Observadas as projeções diárias do enlace dedicado de fibra óptica com largura de banda de 100 Mbps de que dispõe a instituição, verificou-se um pico de exaustão atingido poucas vezes, dispensando, portanto, a hipótese de acréscimo.

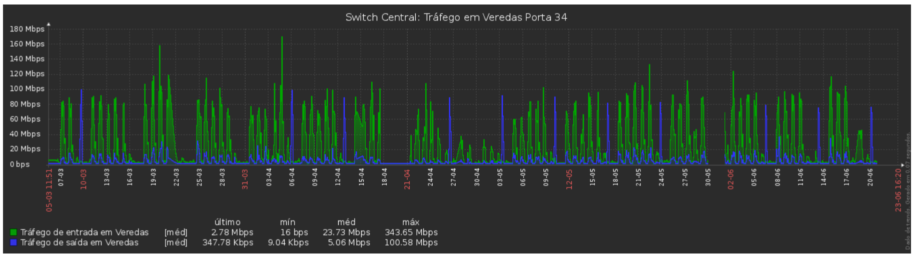

Figura 10. Gráfico de consumo de internet na UFAL Campus Arapiraca [Autor 2020]

5. Conclusão

Uma rede de computadores moderna é composta por um número de dispositivos, serviços e aplicações suficientemente grandes para fugir ao controle de uma gerência puramente humana. Assim, ferramentas automatizadas de gerenciamento de rede são indispensáveis para lidar com esse cenário e, o Zabbix, como plataforma de gerenciamento, se mostrou uma solução viável, sendo de baixo custo, de boa usabilidade e oferecendo uma ampla gama de funcionalidades. Com o Zabbix, a identificação, visualização, correção, antecipação e prevenção de problemas relacionados à rede da instituição, tornou-se possível, melhorando assim a qualidade e disponibilidade dos serviços fornecidos por esta.

Em trabalhos futuros serão abordados estudos sobre o recurso de descoberta de baixo nível (Low-level discovery) [Zabbix 2020] do Zabbix para o mapeamento automático de dispositivos e recursos representados por OIDs contidos em subárvores

SNMP extensas, e a aplicação desse para criação de *templates*. Também serão elaborados estudos para melhoria de desempenho do Zabbix no ambiente de produção da UFAL através do refinamento de configurações [Nelson 2015, p. 23] da ferramenta e de sistemas baseados em GNU/Linux.

Referências

Benicio, W. E. P. (2015). In IF, editor, *Monitoramento e Gerenciamento de Redes utilizando Zabbix*, page 6. Trabalho de conclusão de curso.

Black, T. L. (2008). In UFRGS, editor, *Comparação de Ferramentas de Gerenciamento de Rede*, pages 13–60. Trabalho de conclusão de curso de especialização.

Case, J., Fedor, M., Schoffstall, M. L., and Davin, J. (1990). Rfc1157: Simple network management protocol (snmp). *ACM*, pages 6–7.

Cisco Systems, I. (2004). Internetworking technologies handbook. page 132. Cisco Press, 3th edition.

dos Santos, L. N. and Martins, H. P. (2016). Comparativo das funcionalidades das ferramentas open-source zabbix e cacti. *FATEC,Caderno de Estudos Tecnológicos*, 4(1).

Extreme Networks, I. (2020). How to find oid for a particular mib. Disponível em: https://gtacknowledge.extremenetworks.com/articles/How_To/How-to-find-OID-for-a-particular-MIB. Acesso em: 1 de junho de 2020.

Ford, M., Kim Lew, H., Spanier, S., and Stevenson, T. (1999). Internetworking technology overview. *Cisco Systems, Inc*, pages 45–52.

iReasoning, I. (2020). Mib browser version 13 user guide. Disponível em: http://www.ireasoning.com/browser/help.shtml. Acesso em: 09 de junho de 2020.

Kovacs, K. (2016). Zabbix vs nagios comparison. *Pridobljeno*, 5(5):2016.

Kurose, J. F., Ross, K. W., and Zucchi, W. L. (2013). Gerenciamento de rede. In *Redes de Computadores ea Internet: uma abordagem top-down*, pages 555–572. Pearson Addison Wesley, 6 edition.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., and Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, 39(5):22–31.

Nelson, A. (2015). Tuning the zabbix server. In *Zabbix Performance Tuning*, page 23. Packt Publishing, 1th edition.

Stevenson, D. W. (1995). Network management: What it is and what it isn't. *Carleton University*, 4.

Yemini, Y. (1993). The osi network management model. *IEEE Communications Magazine*, 31(5):20–29.

Zabbix, L. (2020). Zabbix documentation 4.0. Disponível em: https://www.zabbix.com/documentation/4.0/manual. Acesso em: 3 de junho de 2020.