Do Planejamento à Implementação: Adotando uma Ferramenta Open Source em um Ambiente Corporativo

Cristian Kazimirski

Ciência da Computação – Universidade de Passo Fundo (UPF) – Campus I – Passo Fundo – RS

181586@upf.br

Abstract. *This article describes how network monitoring in companies can be a significant challenge, often characterized by a lack of adequate oversight, resulting in performance issues and frequent failures. To address this situation, the open-source tool Zabbix was implemented, standing out for its robustness and flexibility. The main results achieved with the use of Zabbix include notable improvements in service availability, proactive problem detection, and resource optimization, enabling the identification and resolution of issues that previously went unnoticed. This approach not only enhanced operational efficiency but also prepared the infrastructure for future demands.*

Resumo. *Este artigo descreve que o monitoramento de redes em empresas pode ser um desafio significativo, caracterizado pela falta de uma supervisão adequada, o que resulta em problemas de desempenho e falhas frequentes. Para enfrentar essa situação, decidiu-se implementar a ferramenta open source Zabbix, que se destacou por sua robustez e flexibilidade. Os principais resultados obtidos com o uso do Zabbix incluem melhorias notáveis na disponibilidade dos serviços, detecção proativa de problemas e otimização dos recursos, permitindo identificar e corrigir questões que antes passavam despercebidas. Essa abordagem não apenas melhorou a eficiência operacional, mas também preparou a infraestrutura para futuras demandas.*

1. Introdução

O monitoramento de redes tornou-se uma prática indispensável para as empresas modernas, desempenhando um papel crucial na garantia da continuidade dos serviços e na eficiência operacional.

Em um cenário corporativo onde a dependência de sistemas digitais só aumenta, a capacidade de identificar e resolver problemas rapidamente se torna não apenas desejável, mas absolutamente essencial. Isso é fundamental para minimizar interrupções e maximizar a produtividade, pois qualquer falha pode resultar em perdas significativas.

Nos últimos anos, as ferramentas de código aberto têm se destacado no gerenciamento de redes, oferecendo uma série de benefícios que não podem ser ignorados. Essas soluções proporcionam flexibilidade e personalização, permitindo que as organizações adaptem as ferramentas às suas necessidades específicas.

Além disso, a transparência que essas ferramentas oferecem é um ponto forte, pois permite que as empresas compreendam melhor o funcionamento interno das soluções que estão utilizando. Outro aspecto importante é que essas ferramentas costumam ser mais econômicas, ajudando a reduzir os custos operacionais associados ao monitoramento (Maria Fernanda Moge dos Reis, 2023).

Entretanto, a ausência de um sistema eficaz de monitoramento na empresa utilizada neste estudo resultou em falhas frequentes e problemas de desempenho,

comprometendo as operações diárias e a satisfação dos usuários. Longos períodos de inatividade dificultam a identificação das causas dos problemas, evidenciando a urgência de implementar uma solução que seja tanto eficiente quanto adaptável às necessidades específicas da organização. Diante desse cenário, este trabalho teve como objetivo selecionar, implementar e avaliar uma ferramenta de monitoramento que atendesse a critérios fundamentais como escalabilidade, facilidade de uso e suporte da comunidade. A análise dos resultados obtidos visa validar a eficácia da solução escolhida e o impacto positivo sobre as operações da empresa.

2. Trabalhos Relacionados

A seguir, serão apresentados alguns trabalhos que compartilham características alinhadas a este projeto.

Estudos anteriores têm demonstrado a eficácia das ferramentas open source no monitoramento de redes empresariais. Por exemplo, (Paulo Henryck Martins Silva, 2021) enfatiza a importância da integração de recursos avançados de monitoramento com sistemas eficazes de alerta, destacando o Zabbix como uma solução essencial para maximizar a eficiência operacional.

Além disso, (Rodrigo Fraga Mohr, 2012) ressalta os benefícios das ferramentas open source, incluindo flexibilidade, personalização e redução significativa nos custos operacionais associados ao monitoramento.

Uma parte importante do monitoramento da rede envolve o uso do ICMP (Internet Control Message Protocol), que é um protocolo fundamental para a comunicação entre dispositivos em uma rede IP. O ICMP permite o envio de mensagens de erro e informações operacionais sobre o estado da rede, sendo essencial para a detecção de problemas de conectividade. No trabalho de (Danilo Vieira Lopes, 2008), destaca-se a importância do ICMP no monitoramento, enfatizando como ele permite que dispositivos verifiquem a acessibilidade uns dos outros por meio do comando "ping".

Este comando envia pacotes ICMP Echo Request e aguarda respostas ICMP Echo Reply, uma funcionalidade crucial para determinar se um dispositivo está disponível e funcionando corretamente.A implementação do Zabbix neste projeto utilizou o ICMP como uma das métricas principais para monitorar a disponibilidade dos switches e outros dispositivos na rede. Essa abordagem teve como base as diretrizes propostas pelos autores.

Além do ICMP, o SNMP (Simple Network Management Protocol) também desempenha um papel crucial no monitoramento de redes. O SNMP é amplamente utilizado para coletar informações de desempenho e status de dispositivos como switches, roteadores e servidores. Ele permite a gestão e a monitoração remota desses dispositivos, proporcionando uma visão abrangente do estado da infraestrutura de rede assim como apontou (Pedro Eduardo Camera, 2020).

3. Metodologia

No caso de estudo utilizado neste trabalho teve como base a empresa Mig-PLUS Agroindustrial, portanto consideramos um cenário com dois sites distintos. Em cada um deles, há um switch core aos quais correspondem em 4 switchs responsáveis pela distribuição de serviços e comunicação entre os servidores.

Além disso, contamos com 10 switches gerenciáveis em cada prédio, que facilitam a distribuição de internet e serviços para as demais máquinas da infraestrutura. A rede é interligada por uma conexão de fibra óptica, garantindo uma conexão direta entre os switches de cada site, o que proporciona redundância e maior confiabilidade nas comunicações.

A escolha da ferramenta de monitoramento foi baseada em uma análise criteriosa de aspectos que garantem a sua eficácia e adequação às necessidades organizacionais. Os critérios considerados foram:

- Curva de Aprendizado: Avaliou-se o tempo necessário para dominar a ferramenta.Soluções com uma curva de aprendizado mais suave facilitam a adaptação dos usuários,
- Documentação: Qualidade das instruções e guias. Uma boa documentação reduz o tempo de implantação.
- Escalabilidade: Considerou-se a capacidade da ferramenta acompanhar o crescimento das demandas e as necessidades da organização, sem perder desempenho.
- Suporte da Comunidade: Engajamento da comunidade que oferece soluções e suporte informal, especialmente em ferramentas de código aberto.
- Flexibilidade: A possibilidade de personalizar a ferramenta conforme as necessidades específicas da organização.
- Intuitividade: Facilidade de uso da interface. Interfaces intuitivas permitem eficiência desde o início.
- Integração: Capacidade de se conectar com outras ferramentas, melhorando a utilidade e a troca de dados.

3.1 Testes Práticos e Comparação

Foram realizadas análises e testes práticos com diferentes ferramentas de monitoramento, considerando suas principais características, vantagens e limitações. A seguir, um resumo do comparativo das ferramentas avaliadas, destacando seus pontos fortes e fracos.

- Zabbix: Destaca-se pela robustez e flexibilidade, sendo capaz de monitorar redes, sistemas e aplicações em grande escala. Sua interface amigável e documentação detalhada facilitam o uso, tornando-a uma das soluções mais completas do estudo[1].
- Grafana: Apresenta um forte diferencial na visualização de dados, oferecendo gráficos atraentes e personalizados que tornam a análise de métricas mais intuitiva[2]. No entanto, sua funcionalidade depende da integração com outras ferramentas de coleta de dados, como o Zabbix ou Prometheus[3].
- Nagios: Conforme descrito por (OPENSOURCE.COM, 2019), o Nagios é altamente personalizável e oferece um monitoramento eficiente de serviços,

[1] https://www.zabbix.com/
[2] https://grafana.com/
[3] https://prometheus.io/

aplicações e sistemas operacionais. Entretanto, durante os testes, foi identificado um problema crítico de escalabilidade, devido ao alto consumo de recursos necessários para suportar operações em larga escala[4].

- Cacti: Com foco na coleta gráfica de dados via SNMP, o Cacti apresentou simplicidade na configuração e uma interface acessível. Contudo, suas funcionalidades são limitadas em comparação com as demais ferramentas analisadas, tornando-o menos adequado para ambientes que exigem maior flexibilidade e complexidade[5].

Os testes e análises permitiram uma visão abrangente das capacidades e limitações de cada ferramenta, orientando a escolha da solução Zabbix como a mais adequada às necessidades específicas do ambiente monitorado: flexibilidade e capacidade de escalabilidade.

4. Estudo de Caso: Aplicação da Ferramenta

Após a conclusão da instalação e configuração inicial do Zabbix, iniciamos a implementação do Zabbix Agent em todas as máquinas que seriam monitoradas. Entre os dispositivos monitorados, estão servidores que operam com Windows Server 2019, Windows Server 2008 e Ubuntu 22, além de thin clients que estão rodando em Raspberry Pi Model B+ 3.

No ambiente industrial, contamos com IHMs[6] que estão rodando em Windows CE e CLPs, enquanto no escritório há notebooks e desktops aos quais estão rodando em Windows 10 e Ubuntu 22 e Ubuntu 24, totalizando aproximadamente 300 máquinas, todas as quais foram configuradas para monitoramento.

Este processo exigiu um investimento considerável de tempo, especialmente devido à presença de várias máquinas em nosso parque que operam com versões obsoletas de seus sistemas operacionais. Além disso, algumas dessas máquinas apresentavam limitações de espaço, não possuindo 20MB necessários para a instalação do agente.

Para contornar essas dificuldades, foi utilizado o protocolo SNMP (Simple Network Management Protocol) para monitorar o tráfego de rede e o downtime desses equipamentos. Essa abordagem permitiu a identificação de possíveis falhas nas comunicações.

Para a implementação do Zabbix, foi disponibilizada uma máquina virtual Debian GNU/Linux 12, CPU X3430 @ 2.40GHz com 4 núcleos e 4 threads e 4GB de RAM (Zabbix.com, 2024).

Juntamente com a instalação do Zabbix, foram instalados agentes Zabbix em todos os equipamentos, incluindo a configuração do protocolo SNMP em todos os switches. O sistema foi configurado para enviar alertas tanto por e-mail quanto pelo Telegram.

Entre as principais métricas de desempenho que iremos monitorar será a capacidade do disco, evitando assim falhas de serviço devido à falta de espaço. O

---

[4] https://www.nagios.org/
[5] https://www.cacti.net/
[6] Consiste em um monitor touch integrado a um computador, projetado para permitir a interação entre operadores e sistemas industriais ou de automação.

tráfego da rede acompanhando o uso nas interfaces da rede ajuda a identificar congestionamentos ou problemas de largura de banda. Incluindo também o uso de CPU, uso de memória e downtime.

4.1 Monitoramento da Rede

Para monitorar a rede de forma eficaz, foram utilizadas as seguintes configurações, as quais serão detalhadas nos subitens abaixo. Estas se revelaram essenciais para garantir um acompanhamento detalhado e preciso do desempenho dos dispositivos e serviços, não apenas possibilitando a detecção de problemas em tempo real, mas também fornecendo uma visão abrangente da saúde da infraestrutura.

4.1.1. Unavailable by ICMP ping

A expressão apresentada na Figura 1 avalia a acessibilidade do switch via ICMP ping. Para isso, utiliza a função max para determinar o valor máximo do item icmpping nas últimas três tentativas. Caso o valor máximo seja 0, significa que todas as tentativas falharam, indicando a indisponibilidade do dispositivo. Nessa situação, um alerta é gerado para sinalizar que o switch não está respondendo às requisições ICMP.

Figura 1. Métrica utilizada para verificar a acessibilidade

4.1.2. SNMP Data Collection

A expressão apresentada na Figura 2 verifica se a última coleta de dados SNMP também falhou. Se o valor máximo for 0, isso indica que não foi possível coletar dados via SNMP, sugerindo que o dispositivo pode estar offline ou inacessível.Este item depende do estado de disponibilidade do switch via ICMP ping.

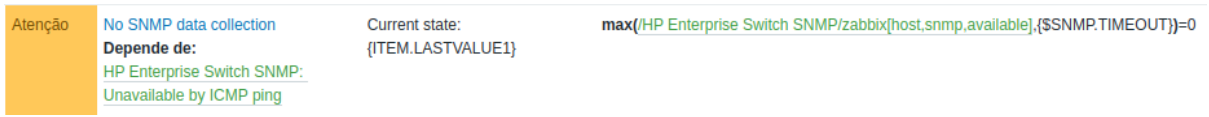

Figura 2. Métrica utilizada para verificar ping

4.1.3. Host has been restarted

A expressão apresentada na Figura 3 ilustra a métrica utilizada para verificar se o switch foi reiniciado recentemente. Esta condição avalia dois cenários: O uptime do sistema (hrSystemUptime) está entre 0 e 10 minutos, indicando um reinício recente. O uptime do sistema é 0 e o uptime da rede (sysUpTime) também é inferior a 10 minutos, sugerindo que o dispositivo foi reiniciado ou desligado.

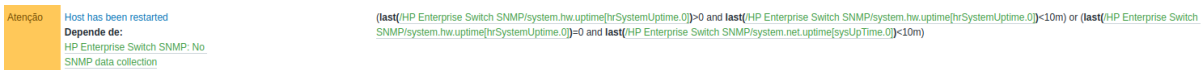

Figura 3. Métrica utilizada para verificar se o switch foi reiniciado

4.1.4. High ICMP ping response time

A expressão apresentada na Figura 4 apresenta a métrica que monitora se o tempo de resposta do ICMP ping está elevado. A condição verifica se a média do tempo de resposta dos pings (icmppingsec) nos últimos 5 minutos excede um valor de aviso de 100 ms a 300 ms definido pelo ({$ICMP_RESPONSE_TIME_WARN}). As dependências indicam que essa verificação deve ser considerada apenas se houver uma

alta perda de pacotes ou se o dispositivo estiver indisponível por ICMP.

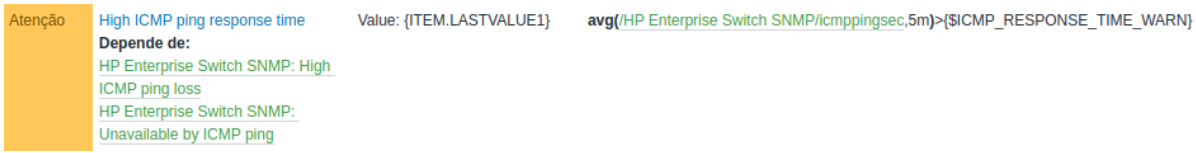

Figura 4. Métrica utilizada para verificar o tempo de resposta

4.1.5. High ICMP ping loss

A expressão apresentada na Figura 5 ilustra a métrica utilizada para avaliar a perda de pacotes durante os testes de ping. A condição verifica se a perda mínima de pacotes (icmppingloss) nos últimos 5 minutos é maior que um limite de aviso definido ({$ICMP_LOSS_WARN}) e menor que 100%. As dependências indicam que essa verificação deve ser considerada somente se o dispositivo estiver indisponível por ICMP.

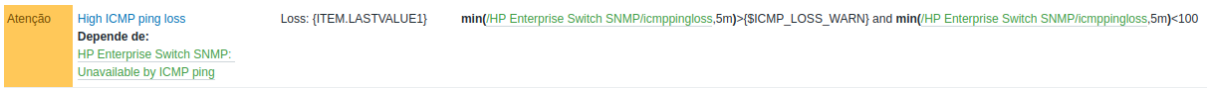

Figura 5. Métrica utilizada para verificar a perda de pacotes

4.2 Alertas e Notificações

Os alertas são enviados por meio de dois canais principais: e-mail e Telegram. Essa abordagem multicanal permite que a equipe de operações receba notificações instantâneas, independentemente da localização ou do dispositivo que estiver utilizando. Além dos alertas por e-mail e Telegram, utilizamos um dashboard centralizado que fornece uma visão abrangente do estado da infraestrutura.

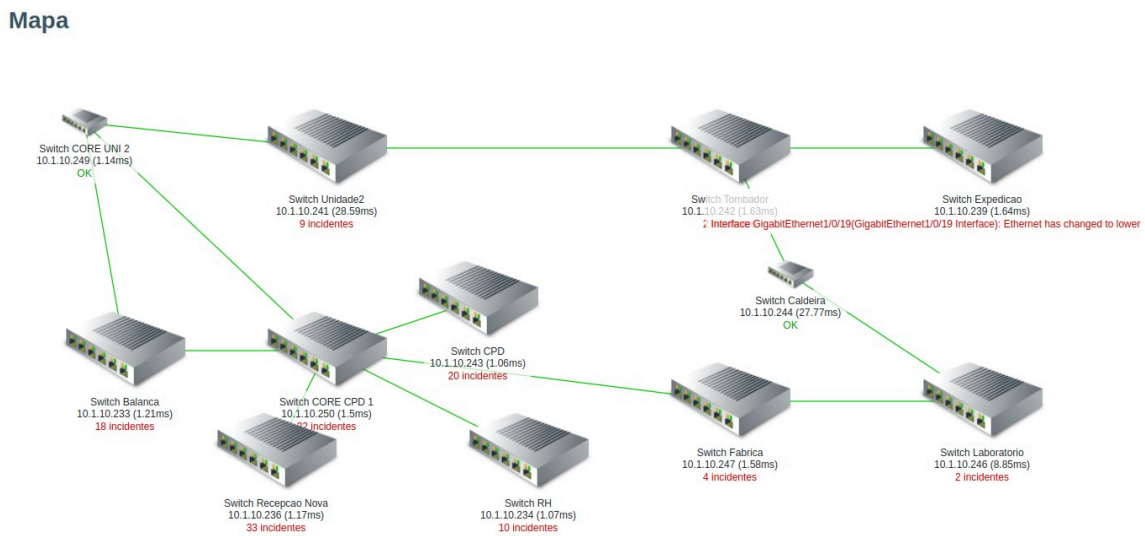

Figura 6. Mapa de rede com ligações

A Figura 6 apresenta um mapa de rede que ilustra as conexões entre os switches monitorados. Esta visualização é essencial para a identificação rápida de problemas, pois permite que a equipe visualize a topologia da rede e localize facilmente onde as falhas estão ocorrendo.

Figura 7. Dashboard de eventos

Na Figura 7 é exibido o dashboard de eventos, que centraliza todas as informações relevantes sobre o estado da rede em tempo real. Este dashboard é projetado para exibir alertas, métricas de desempenho e outros dados críticos, permitindo que a equipe monitore a saúde da infraestrutura de forma contínua.

Para garantir que todos na equipe estejam cientes das condições críticas, foi disponibilizada uma televisão na qual o dashboard é exibido. Essa tela não apenas mostra os dados em tempo real, mas também emite alertas sonoros para notificar sobre severidades dos problemas, assegurando que a equipe esteja sempre informada sobre quaisquer incidentes que possam afetar o desempenho da rede.

Essa implementação robusta de monitoramento e notificação é fundamental para manter a operação eficiente e minimizar o tempo de inatividade, permitindo uma resposta rápida a qualquer anomalia detectada na infraestrutura.

5. Resultados e Discussão

Após a implementação da ferramenta Zabbix, foram notáveis as melhorias alcançadas no monitoramento e gestão da infraestrutura. As principais mudanças percebidas, no período de 2 meses após a implementação, serão abordadas nos seções abaixo.

5.1 Disponibilidade de serviços

Antes da adoção do Zabbix, a equipe de TI enfrentava sérias dificuldades para identificar problemas rapidamente, o que resultava em longos períodos de inatividade que afetam a produtividade e a eficiência operacional da empresa.

A situação se agrava pela falta de um sistema de monitoramento eficaz, que tornava quase impossível detectar falhas antes que elas causassem impactos significativos nos processos da organização.

Com a implementação do monitoramento proporcionado pela ferramenta Zabbix, foi possível não apenas detectar problemas em tempo real, mas também resolvê-los antes que afetasse de forma crítica as operações da empresa.

Um exemplo ilustrativo ocorreu durante o período de monitoramento, quando foi registrado um evento crítico em que o Switch Balança deixou de se comunicar. Este incidente, que aconteceu no dia 24 de outubro, teve um impacto direto na conectividade de 18 dispositivos conectados à rede, evidenciando a importância do monitoramento contínuo e proativo.

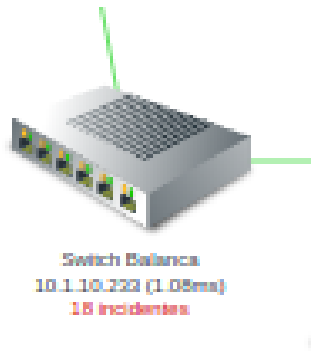

Figura 8. Notificação do incidente

Na Figura 8 é ilustrado como se dá a notificação do incidente, destacando a rapidez com que a equipe foi alertada sobre o problema. Graças à detecção imediata do Zabbix, foi possível atender às demandas de cada um dos usuários de maneira mais assertiva e eficiente, economizando tempo na identificação do real problema por trás das solicitações feitas.

Uma investigação mais aprofundada revelou que a causa raiz do problema estava relacionada à falta de energia elétrica, provocada por um incêndio no painel elétrico, este evento não apenas sublinhou a importância da monitoração contínua da rede, mas também demonstrou a capacidade do Zabbix em detectar problemas críticos antes que eles se tornassem uma crise maior.

A experiência reforçou a necessidade de um sistema robusto de monitoramento para garantir que interrupções como essa possam ser rapidamente identificadas e resolvidas, mantendo assim a continuidade dos serviços e a satisfação dos usuários.

5.2 Detecção do desempenho da rede

Com essa nova abordagem de detecção, tornou-se possível identificar situações que poderiam facilmente passar despercebidas em um monitoramento convencional.

Um exemplo notável foi a constatação de que uma máquina virtual (VM) estava apresentando um tráfego muito acima do normal, o que resultou em uma notificação imediata por parte do Zabbix. Essa notificação não apenas chamou a atenção da equipe, mas também serviu como um alerta crítico para investigar mais a fundo o que estava acontecendo.

Ao analisar essa situação específica, ficou claro que uma aplicação utilizada dentro da fábrica estava realizando uma quantidade excessiva de requisições ao banco de dados instalado nessa máquina virtual.

Essa sobrecarga resultou em lentidão significativa em outros serviços que dependiam dessa mesma VM, criando um efeito cascata que afetou a produtividade geral. A situação ilustra perfeitamente como um monitoramento eficaz pode revelar problemas ocultos antes que eles se tornem críticos.

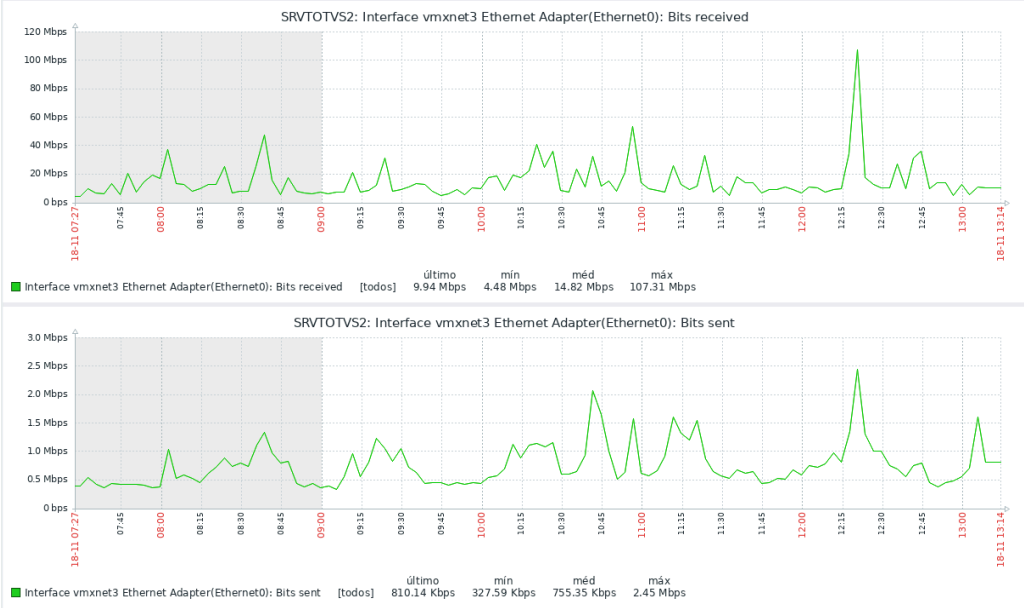

Figura 9. Gráfico do fluxo

Na figura 9 são apresentados gráficos do fluxo de dados mencionados acima, evidenciando o aumento anômalo no tráfego e permitindo uma visualização clara do problema. Podemos visualizar um claro pico anômalo, enquanto a máquina não possui desempenho para entregar tudo que foi solicitado.

Após essa ocorrência, a equipe decidiu realizar uma reformulação no programa responsável pelas requisições ao banco de dados. Essa mudança foi crucial para evitar que o problema se repetisse no futuro e para garantir que os serviços continuassem a operar de maneira eficiente e sem interrupções.

5.3 Otimização de recursos

Durante a análise do ambiente de trabalho, identificamos que várias máquinas dos usuários estavam operando em modo Half-Duplex. Essa notificação foi ocasionada por cabos de rede danificados e condições de ruído na rede podem ser observadas na Figura 10. Essa configuração, que permite a transmissão de dados em apenas uma direção por vez, gerou um impacto significativo na performance, especialmente considerando que todas essas máquinas são thin clients.

Figura 10. Notificação da incidência da porta 35 operando em half-duplex

Como resultado dessas ações, observamos uma melhoria significativa no desempenho das máquinas. Os usuários relataram uma experiência mais fluida e eficiente, com redução nos tempos de espera e aumento na produtividade. Essa otimização não apenas melhorou o ambiente de trabalho, mas também reforçou a importância de seu monitoramento.

5.4 Análise dos resultados

A implementação dos dashboards no ambiente trouxe à tona informações cruciais sobre a performance das máquinas e sistemas utilizados, especialmente em relação ao ERP utilizado pela empresa.

Durante a análise, observou-se que a máquina responsável pelo gerenciamento do ERP estava lidando com um volume excessivo de requisições, o que compromete sua capacidade de processamento integrado. Essa situação gerava atrasos e ineficiências que impactavam diretamente as operações da empresa.

Com os dados coletados e apresentados de forma clara através dos dashboards, a direção decidiu investir na compra de um servidor mais robusto, capaz de atender à crescente demanda e melhorar a eficiência do processamento das requisições de ERP.

Os resultados também evidenciaram a necessidade urgente de reformulação na infraestrutura de redes da empresa. Essa reforma está prevista para ocorrer, visando não apenas resolver problemas atuais, mas também preparar a empresa para futuras expansões e necessidades operacionais.

5.5 Desafios encontrados

Durante o processo de implementação do Zabbix para monitoramento das máquinas, um dos principais desafios enfrentados foi a necessidade de instalar o Zabbix Agent em cada um dos equipamentos individuais. Onde consistia em executar o instalador do agente, após o término da instalação era configurado o arquivo zabbix_agentd.conf para definir o servidor e o hostname.

Essa tarefa, que à primeira vista pode parecer simples, revelou-se bastante demorada e complexa, especialmente devido à grande quantidade de máquinas envolvidas no projeto e às condições nem sempre ideais em que algumas delas operam. A instalação manual em cada dispositivo não apenas consumiu um tempo considerável, mas também exigiu uma coordenação meticulosa para garantir que todas as máquinas fossem devidamente configuradas e integradas ao sistema de monitoramento.

Além disso, a diversidade dos sistemas operacionais e as limitações de hardware de algumas máquinas tornaram o processo ainda mais desafiador. Cada etapa da instalação demandou atenção especial para evitar erros.

Para otimizar esse processo em futuras implementações, seria extremamente vantajoso desenvolver uma solução que permita a instalação do cliente do Zabbix de forma autônoma.A criação de um script ou a utilização de ferramentas de automação que possibilitem a instalação do Zabbix Agent em múltiplas máquinas simultaneamente não só reduziria significativamente o tempo necessário para essa tarefa, mas também minimizaria o esforço humano envolvido, permitindo que a equipe se concentre em outras atividades críticas.

Essas abordagens, acima mencionadas, não apenas tornaram o processo mais eficiente, mas também garantiriam uma configuração mais uniforme e precisa em toda a infraestrutura.

6. Conclusão

Com base nos resultados obtidos, podemos concluir que o monitoramento de redes em um contexto corporativo não é apenas importante, mas essencial para que a equipe

trabalhe de maneira mais eficiente. Este experimento destacou que o monitoramento constante da rede é primordial para a fluidez de uma empresa.

A implementação de ferramentas Open Source traz não apenas economia para a empresa, mas também benefícios duradouros para a comunidade como um todo (Evila Piva, 2019).

Essa abordagem resultou em melhorias significativas na disponibilidade dos serviços, na detecção proativa de problemas e na otimização de recursos. Com o Zabbix, conseguimos identificar e corrigir questões que antes passavam despercebidas, fazendo isso de forma mais assertiva e sem comprometer o desempenho da infraestrutura.

Apesar dos resultados positivos, ainda existem áreas que podem ser aprimoradas. Por exemplo, seria valioso desenvolver uma opção que otimize a instalação do cliente Zabbix e implementar automações para respostas a falhas, o que poderia aumentar ainda mais a eficiência do sistema. Essas melhorias não apenas facilitarão futuras implementações, mas também garantirão um monitoramento ainda mais eficaz e responsivo.

Por fim, vale ressaltar que a experiência trouxe a perspectiva de que há a importância de continuar investindo em melhorias e inovações no monitoramento da infraestrutura de TI. Em ambientes empresariais, onde a conectividade e o desempenho dos sistemas são fundamentais para as operações diárias, o monitoramento contínuo garante a identificação precoce de falhas, evitando interrupções que podem gerar prejuízos financeiros. Além disso, o acompanhamento proativo possibilita uma gestão mais eficiente dos recursos, assegurando que a infraestrutura atenda às demandas do negócio com confiabilidade e desempenho otimizados. Investir em soluções de monitoramento é, portanto, uma estratégia essencial para manter a competitividade e a resiliência no mercado corporativo.

7. Referências

Danilo Vieira Lopes, Jaime Batista do Santos (2008). Análise Estatística da Latência e Perda de Pacotes numa Redes de Computadores. Disponível: https://www.dimap.ufrn.br/~sbmac/ermac2008/Anais/Resumos%20Estendidos/Analise%20estatistica_danilo.pdf. Acesso: novembro/2024.

Evila Piva, Francesco Rentocchini, Cristina Rossi‐lamastra (2019). Is Open Source Software about Innovation? Collaborations with the Open Source Community and Innovation Performance of Software Entrepreneurial Ventures. Disponível: https://www.tandfonline.com/doi/abs/10.1111/j.1540-627X.2012.00356.x. Acesso: novembro/2024.

Maria Fernanda Moge dos Reis, Cassiano Nakaoka, Geraldo Henrique Neto (2023). DESENVOLVIMENTO DE UMA PIPELINE DE DADOS UTILIZANDO SOLUÇÕES OPEN-SOURCE EM UM AMBIENTE DE BIG DATA. Disponível: http://periodicos.unifacef.com.br/reca/article/view/2776. Acesso: novembro/2024.

OPENSOURCE. Top 5 open source network monitoring tools. Disponível: https://opensource.com/article/19/2/network-monitoring-tools. Acesso: Outubro/2024.

Paulo Henryck Martins Silva (2021). GERENCIAMENTO DE REDES COM ZABBIX. Pontifícia Universidade Católica de Goiás, 2021.

Pedro Eduardo Camera (2020). INT FLOW: APLICAÇÃO DE TELEMETRIA EM REDES DEFINIDAS POR SOFTWARE, 2020

Rodrigo Fraga Mohr (2012). Análise de Ferramentas de Monitoração de Código Aberto. Universidade Federal do Rio Grande do Sul, 2012.

ZABBIX 7.0 (2024). Documentation manual – Requirements. Disponível: https://www.zabbix.com/documentation/current/en/manual/installation/requirements. Acesso: novembro/2024.