

Proposta de Monitoramento de Rede para a Prefeitura Municipal de São Sepé Utilizando a Ferramenta Zabbix

Jefferson dos Santos Corrêa¹, Gustavo Stangherlin Cantarelli¹

¹Curso de Sistemas de Informação – Universidade Franciscana
CEP 97010-032 – Santa Maria – RS – Brasil

jeffs_correa@hotmail.com, gus.cant@gmail.com

Abstract. *The present work proposes the implementation of a Zabbix network monitoring system for the city of São Sepé - RS. This system has the development of scripts and templates to complement missing features in Zabbix, using the programming language Shell Script. Also, the development of dashboards for reports with the Grafana tool, in order to improve IT management and user interaction with the information collected from the network environment. Subsequently, performance tests will be performed to check the band and the performance of data connections.*

Resumo. *O presente trabalho propõe a implantação de um sistema de monitoramento de rede Zabbix para a prefeitura de São Sepé - RS. Sistema este que possui desenvolvimento de scripts e templates para complementar funcionalidades ausentes no Zabbix, utilizando a linguagem de programação Shell Script. Também, o desenvolvimento de dashboards para relatórios com a ferramenta Grafana, a fim de aprimorar a gestão TI e a interação do usuário com as informações coletadas do ambiente de rede. Posteriormente, foram feitos testes de desempenho para verificação da banda e a performance de conexões de dados.*

1. Introdução

A cada ano, novas aplicações e novos usuários impulsionam o crescimento das redes de computadores, tanto em escala quanto em complexidade. A necessidade de monitorar e gerenciar essas redes perante o seu crescimento exige também o desenvolvimento cada vez mais aprimorado de softwares e técnicas para acompanhar as novas tecnologias lançadas no mercado.

Com essa expansão, tanto de dispositivos como de equipamentos de rede, faz com que os serviços de tecnologia de informação, que atuam em organizações públicas, dependam ainda mais das redes de computadores para seu funcionamento [Black 2008].

Conforme Silva, Medeiros e Martins (2015), o orçamento operacional, principalmente os custos com pessoal e os custos operacionais associados à manutenção dos sistemas de informação, representa 70% de todo o gasto de TI em uma empresa. Com o fato de o cotidiano das pessoas estar relacionado diretamente com as redes de computadores, manter o serviço de TI conforme o esperado, sem um gerenciamento eficaz, é complicado até mesmo em ambientes de pequeno porte.

Existem várias ferramentas de monitoramento disponíveis no mercado, contudo, para este trabalho, foi utilizada a ferramenta Zabbix por sua flexibilidade e capacidade de

monitorar todo o ambiente de rede, tanto hardware quanto software. Possuindo uma interface web agradável e um sistema de banco de dados relacional, possibilita que as informações armazenadas possam ser consultadas, gerando gráficos e outros formatos visuais.

Não é de hoje que as redes de computadores vêm se tornando cada vez maiores e mais importantes nas empresas. Junto com isso, aumenta a responsabilidade do analista de rede em monitorar e garantir a segurança e o funcionamento dos diversos dispositivos trafegando dados na rede. Ao planejar um monitoramento adequado para a empresa, o analista pode acompanhar a “saúde da rede” e, principalmente, antecipar possíveis falhas ou quedas de performance. Esses problemas geralmente resultam em menor produtividade dos setores que dependem do departamento de TI.

Partindo desse princípio, foi constatada a insuficiência do monitoramento presente na rede interna da Prefeitura Municipal de São Sepé - RS. Sendo a prefeitura o principal órgão de serviços de um município, é de extrema importância garantir a disposição dos serviços e a segurança dos dados dos cidadãos.

1.1. Objetivo geral

O objetivo deste trabalho é propor a implantação da ferramenta Zabbix para o monitoramento dos dispositivos de rede presentes na prefeitura de São Sepé. E, por meio da linguagem de programação Shell Script, implementar *scripts* e *templates* para alcançar um melhor gerenciamento dos ativos de rede e garantir um sistema de monitoramento eficiente e proativo. Também, foi utilizado a integração da ferramenta Grafana, com intuito de melhorar a visualização das informações armazenadas pelo sistema.

1.2. Objetivos específicos

Para este trabalho, os objetivos específicos encontrados são:

- Utilizar o Sistema Operacional CentOS 8 x64;
- Fazer uso da Ferramenta Zabbix versão 4.4 para monitoramento;
- Instalar e configurar o Servidor Zabbix e Agente Zabbix;
- Utilizar o Grafana para visualizar e personalizar gráficos;
- Utilizar o Telegram para os encaminhamentos dos alertas do Zabbix
- Monitorar a infraestrutura, a fim de reduzir falhas na segurança dos dados;
- Garantir a atualização em tempo hábil dos estados dos serviços monitorados;
- Estudar e implementar *scripts* e *templates* para facilitar a operação do ambiente, e a melhor prática de trabalhar com o Zabbix;
- Realizar testes de performance na rede;

2. Referencial Teórico

Nesta seção, serão abordados tópicos e conceitos dos conteúdos necessários para a fundamentação do trabalho proposto. Também serão apresentadas as tecnologias e ferramentas utilizadas para a implantação do projeto.

2.1. Infraestrutura de redes em órgãos públicos

A cada dia que passa, a demanda por recursos de TI aumenta consideravelmente, sendo assim, uma boa gestão e segurança é imprescindível para os órgãos públicos, visto que essas instituições costumam armazenar dados sigilosos.

A carência em estruturas de TI, e até mesmo de profissionais capacitados, torna ainda mais difícil a integração das entidades públicas com os novos recursos tecnológicos. Dados divulgados pelo G1 mostram que 80% dos municípios não conseguiram integrar o sistema de prontuário eletrônico, relatando que sua infraestrutura de TI é a principal barreira que impede a integração, já que não é capaz de suportar o novo sistema [Figueiredo 2016].

Muitas vezes as prefeituras não possuem um PDTI (Plano Diretor de Tecnologia da Informação) e gerenciam o departamento sem qualquer padronização ou norma. Isso ocasiona uma desordem na gestão dos ativos de TI e resulta em gastos desnecessários com manutenção e contratação de serviços [Figueiredo 2016].

Situações como a citada anteriormente também se manifestam na prefeitura de São Sepé, que, por apresentar uma infraestrutura de pequeno porte, não lhe é dada a devida importância. Sua infraestrutura lógica e física apresenta carência em diversos aspectos, como: equipamentos de rede, cabeamento, planejamento e sistema de monitoramento de rede. Boa parte disso é em razão do procedimento administrativo realizado para contratação de serviços e aquisição de produtos, uma vez que os produtos ou serviços que são selecionados pela licitação nem sempre são os melhores, mas sim os mais baratos.

Embora tenha havido progresso na infraestrutura de rede da prefeitura, ela ainda carece no quesito de detectar e solucionar as falhas encontradas na rede, já que o departamento de TI trabalha de forma reativa e sem uma metodologia fixa ou documentação dos erros e falhas encontradas.

2.2. Gerenciamento de redes

O gerenciamento de rede vem se tornando cada vez mais complexo, em boa parte pelo fato do crescimento exponencial das mesmas tanto em desempenho quanto em suporte a grandes conjuntos de serviços. Além disso, os sistemas de telecomunicação fazem-se presentes e componentes essenciais na rede, também acarretando no aumento de sua complexidade até mesmo em pequenas empresas.

O gerenciamento de redes de computadores pode ser definido como a coordenação (controle de atividades e monitoração de uso) de recursos materiais (modems, roteadores etc.) e ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações [Pinheiro 2002 p. 9].

Os dados que trafegam em uma rede de computadores devem ser transportados de modo a garantir sua agilidade e confiabilidade. Para que isso ocorra, é imprescindível que as informações monitoradas sejam cuidadosamente analisadas de modo que possíveis problemas possam ser detectados e solucionados rapidamente e com eficiência. A rede que não dispõe de uma ferramenta de gerência pode apresentar problemas que afetarão o tráfego dos dados, assim como sua integridade, através de problemas de congestionamento na rede, recursos sobrecarregados entre outros [Pinheiro 2002].

De acordo com Bahls (2016), a arquitetura geral que compõe os sistemas de gerenciamento de rede pode ser determinada por quatro componentes básicos: elementos gerenciados, estações de gerência, protocolos de gerência e informações de gerência.

Elementos gerenciados são os que possuem um software específico chamado de agente, que permitem que os equipamentos possam ser monitorados e controlados por intermédio de uma ou mais estações de gerência.

Estações de gerência são chamados de gerentes, que, por meio de softwares, se comunicam diretamente com os agentes instalados. Essa comunicação pode ter como objetivo tanto monitorá-los como também os controlar, utilizando uma interface fornecida pela estação de gerência.

Já o protocolo de gerência é definido por uma linguagem em comum entre gerente e agente, que permite o monitoramento e controle. E a informação de gerência refere-se aos dados que podem ser referenciados em operações do protocolo de gerência, ou seja, dados dos quais o gerente e o agente se comunicam. A Figura 1 ilustra os principais componentes da arquitetura de gerenciamento de rede.

2.3. Protocolo SNMP (*Simple Network Management Protocol*)

O protocolo SNMP foi desenvolvido para facilitar o monitoramento e gerenciamento de redes, permitindo que uma ferramenta de gerenciamento possa trabalhar com produtos e serviços de diversos fabricantes.

Ele se trata de um protocolo definido a nível de aplicação, segundo o modelo OSI (*Open System Interconnection*). É utilizado para obter informações dos itens a serem monitorados. O item a ser monitorado é considerado como agente; sendo o gerente quem consulta ou solicita modificações por meio do protocolo de transporte UDP e que permite a abstração das outras camadas e o gerenciamento de dispositivos que estejam fora da rede de origem.

Este protocolo é conhecido por ser simples e robusto, além de ser capaz de gerenciar até mesmo redes heterogêneas. Como o processamento de dados fica com o gerente, é consumido poucos recursos da rede e de processamento [Gomes 2017].

2.4. Management Information Base (MIB)

A MIB é uma coleção de objetos de rede gerenciáveis. Esses objetos são uma representação lógica dos componentes físicos de rede habilitados para o protocolo SNMP. Eles guardam informações sobre a configuração desses componentes de rede, como versão do software, endereço IP ou o número da porta e a quantidade de espaço para armazenamento em disco. Seu funcionamento se equivale a um tipo de diretório que contém os nomes lógicos dos recursos de rede e seus parâmetros de configuração gerenciados pelo SNMP [Campos 2018].

2.5. Shell Script

O Shell Script é utilizado no desenvolvimento de arquivos de *scripts* para simplificar tarefas que são executadas repetidamente. Como, por exemplo, a automatização da inicialização de um programa e o esvaziamento da lixeira e diretórios temp para economizar espaço de armazenamento.

Um *script* é um algoritmo criado para realizar determinadas tarefas, usando comandos específicos do bash e executáveis do sistema operacional. Além de poupar muito tempo do programador, possui uma sintaxe simples, permitindo processar desde pequenas quantidades de dados até executar tarefas mais complexas [Lousada 2015].

Segundo Muxfeldt (2017), o Shell é um interpretador de comandos que proporciona uma interface entre o usuário e o sistema operacional. A interface Shell atua como um intermediário, cuja função é ler a linha de comando, interpretar seu significado, executar o comando e devolver o resultado pelas saídas.

2.6. Zabbix

O Zabbix é uma ferramenta de código aberto que monitora diversos parâmetros de ativos de rede que suportem serem acessados remotamente por um endereço IP. Possui mecanismos de alertas e notificações bastantes flexíveis que possibilitam avisar a ocorrência de eventos por meio de SMS, e-mail e aplicativos.

A arquitetura do Zabbix é estruturada em três camadas: aplicação, banco de dados e interface web. Na aplicação é realizado a coleta de dados, no qual o agente Zabbix fica encarregado de reunir as informações dos vários dispositivos presentes na rede que se reportam por meio do protocolo SNMP. A camada de banco de dados é responsável pelo armazenamento das informações coletadas, tarefa efetuada pelo servidor Zabbix. E a camada de interface web (*front-end*) é onde o administrador pode visualizar todos os dados adquiridos na camada de aplicação e fornecem também informações para aplicações que utilizam a API do Zabbix [Lima 2014].

2.6.1. Servidor Zabbix

É o servidor responsável por realizar o armazenamento dos dados coletados em uma base de dados. Pode atuar de duas maneiras diferentes, sendo elas: passivamente, no qual não há a necessidade de um agente para coleta de dados, pois ele realiza a consulta diretamente aos dispositivos monitorados; e ativamente, apenas analisando e armazenando os dados obtidos pelo Agente e Proxy [Lima 2014].

2.6.2. Agente Zabbix

O Agente Zabbix é o encarregado de reunir as informações dos vários dispositivos presentes na rede que se reportam por meio do protocolo SNMP. Foi desenvolvido para ter um baixo consumo de recursos computacionais e não impactar no ambiente monitorado [Lima 2014].

2.7. Grafana

O Grafana é uma ferramenta de código aberto utilizada para visualizar e analisar métricas por meio de gráficos. Possibilita a criação de *dashboards* dinâmicos, além de permitir configurar alertas com base nas métricas definidas pelo usuário.

Com o Grafana, é possível acompanhar e organizar diversas informações importantes, através de uma única interface intuitiva e completa. Com isso, facilita a gestão e o monitoramento de dados, o que torna a tomada de decisões na empresa mais rápida e eficiente.

Embora tenha inúmeros recursos à disposição, a estrutura do Grafana é leve e flexível, já que permite organizar dados vindos de diversas fontes em um mesmo *dashboard*. Além disso, a plataforma é de fácil instalação e permite a integração com banco de dados e outras ferramentas. Todas essas integrações são obtidas através de *plugins* instalados e gerenciados de forma simples na ferramenta [Gomes 2019].

2.8. iPerf3

O iPerf3 é uma ferramenta que realiza medições ativas para determinar a largura de banda e a performance de conexões de dados. Ele suporta ajustes de vários parâmetros relacionados a tempo, protocolos e *buffers*. Para cada teste, ele mede a taxa de transferência e perda de pacotes, entre outros parâmetros.

O iPerf3 foi desenvolvido pelo ESnet/Lawrence Berkeley National Laboratory, não compartilhando o código de suas versões anteriores. Liderado sob uma licença BSD de três cláusulas [iPerf 2020].

2.9. Telegram

O Telegram é um aplicativo de mensagens instantâneas armazenadas em nuvem, que contém uma variedade de recursos tornando-o uma excelente opção para se ter um contato mais próximo e ágil com o cliente. Ele possui métodos bem eficiente para que administradores de grupos possam automatizar mensagens por meio de robôs, trazendo uma série de *bots* programados e possibilitando a configuração de diversas funções para atender as necessidades específicas do negócio [Rocha 2020].

3. Trabalhos Correlatos

Nesta seção serão apresentados trabalhos que auxiliaram no desenvolvimento deste trabalho final de graduação, no qual apresentam estudos e comparativos relacionados às ferramentas de monitoramento e à necessidade de sua aplicação.

3.1. Monitoramento de rede utilizando Zabbix

O trabalho desenvolvido por Maldonado (2016) teve como objetivo mostrar a importância de possuir um software de gerenciamento de rede, não interessando o porte da empresa. No estudo, é apresentada a ferramenta de monitoramento Zabbix e realizados testes simulados em ambientes virtuais.

O autor apresenta brevemente testes nos cinco modelos de gerência de rede, criando alguns *triggers* (gatilhos) para notificar e enviar alertas sobre o uso de hardware dos computadores, uso da internet e erros detectados nos logs de segurança.

Por fim, o autor conclui que o Zabbix é uma ferramenta robusta e capaz de suportar qualquer cenário de redes de computadores, desde os mais simples até os mais complexos e dinâmicos.

3.2. Monitoramento e segurança: uma abordagem sobre como o Zabbix pode contribuir com relação à segurança e à gestão de suas melhores práticas em tecnologia de informação

O projeto apresentado por Alvarenga (2015) identifica, através de relatórios, que os órgãos governamentais são os mais afetados por ataques cibernéticos. Assim, realizando

um estudo mais aprofundado na Câmara Municipal de Campinas, é proposta uma ferramenta de monitoramento, uma vez que ela não possuía nenhum tipo de monitoramento.

Com a necessidade de uma solução de código aberto, confiabilidade e facilidade de aprendizagem, foi optado pela ferramenta de monitoramento Zabbix, pelo fato de ser uma ferramenta considerada mais completa e flexível comparada com seus concorrentes (Nagios, Cacti e ZenOSS).

No trabalho, o autor conclui, após testes e mapeamentos da rede, a viabilidade e os benefícios agregados principalmente ao departamento de TI. Por sua vez, passou de uma administração reativa para proativa, com uma maior eficiência na correção e documentação de eventuais problemas na rede, finalizando, assim, o projeto com a implementação da ferramenta.

3.3. Análise comparativa entre ferramentas para gerenciamento e monitoramento de redes

O trabalho proposto por Andreoli (2016) teve como objetivo realizar uma análise comparativa em três ferramentas gratuitas de monitoramento (Cacti, OMD e Zabbix). Abordou-se o gerenciamento de falhas e o gerenciamento de desempenho, tendo em vista encontrar a melhor solução para o cenário em que as ferramentas foram implantadas.

As três ferramentas analisadas foram submetidas individualmente por sete dias a testes, sobre os critérios avaliativos de: instalação das ferramentas, configuração de *hosts* e serviços e geração de informações claras e objetivas.

As métricas definidas pelo autor foram: grau de dificuldade durante a instalação, necessidade de pacotes adicionais, tempo de instalação, autodescoberta de *hosts*, criação de regras de monitoramento, agente próprio, grau de dificuldade na configuração, mapas e diagramas de rede, geração de gráficos e notificações.

Através dos resultados obtidos com esse trabalho, concluiu-se que a ferramenta mais adequada para o cenário em questão foi o Zabbix, em seguida o OMD e, por último, o Cacti.

Entretanto, esse estudo serviu para determinar a solução mais adequada para a rede do programa Cidade Digital do Município de São Lourenço do Oeste - SC e ainda auxílio ao provedor de internet no qual foram realizados os testes.

3.4. Conclusão sobre os trabalhos correlatos

A partir dos trabalhos pesquisados, observou-se que cada um possui determinada particularidade, porém todos favorecem o uso do Zabbix perante os demais softwares de monitoramento e gerenciamento de rede.

O trabalho de Alvarenga (2015) assemelha-se a este, no fato de propor a ferramenta Zabbix como solução de monitoramento a um órgão público. E, então, serão realizados estudos e testes com a ferramenta, viabilizado seu uso para o ambiente proposto.

Os estudos realizados por Andreoli (2016) foram essenciais para o desenvolvimento deste trabalho, pois expõe três softwares de monitoramento diferentes

sob métricas e critérios de avaliação, de modo a classificar seus pontos positivos e negativos, adequando a solução ideal para o cenário proposto.

Maldonado (2016) apresenta as utilidades e mecanismos de funcionamento do Zabbix, agregando conhecimentos substanciais sobre a ferramenta e suas diversas funcionalidades.

Todos os trabalhos apresentados foram importantes para o desenvolvimento deste projeto, que se destaca entre os outros por propor o uso da ferramenta Zabbix, juntamente com o desenvolvimento de *scripts* e *templates* para complementar e otimizar seu gerenciamento.

4. Metodologia

Com a finalidade de atingir os objetivos do presente trabalho, este foi dividido em quatro fases de execução. Compreende, inicialmente, na análise e configuração do ambiente de rede; planejamento da implementação baseado nos requisitos funcionais e não funcionais; representação do fluxo de execução do sistema; e, para finalizar, foram efetuados testes de desempenho, utilizando a ferramenta Iperf3, para verificar a banda e a performance de conexões de dados.

4.1. Análise e configuração do ambiente de rede

Nesta fase foram analisados e definidos os equipamentos e itens essenciais para o monitoramento como também realizada a instalação e configuração do ambiente Zabbix.

Os equipamentos monitorados foram: nove impressoras, um roteador, um servidor de dados, um servidor web e o servidor do Zabbix. Na Figura 4 é apresentando a topologia da rede, com os respectivos hosts monitorados.

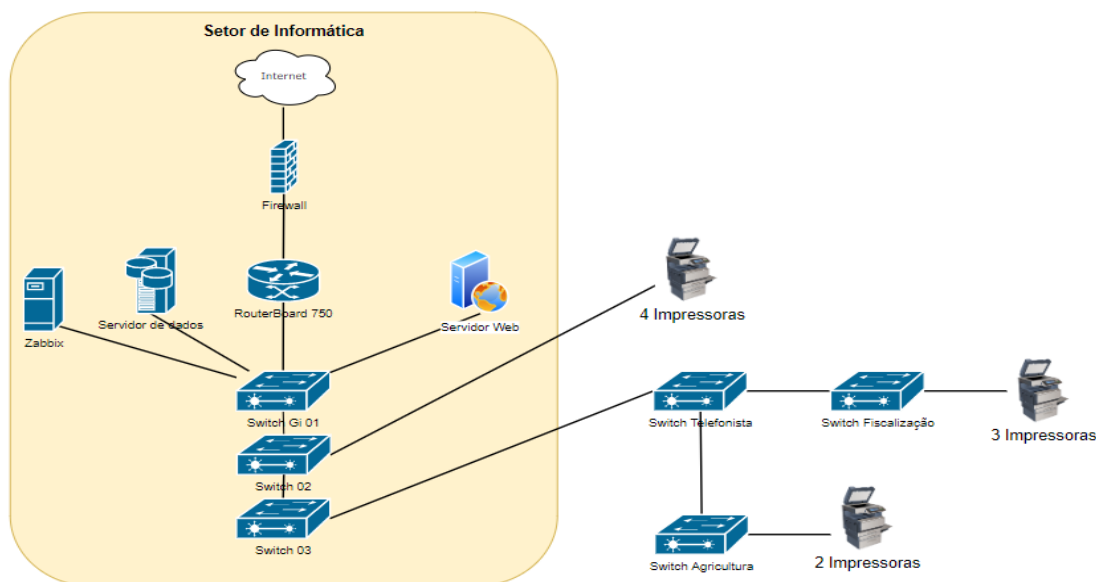


Figura 4. Topologia de rede da prefeitura.

A configuração do ambiente de rede obteve-se, inicialmente pela instalação do software Virtual Box e do sistema operacional CentOS 8. Para a instalação da ferramenta Zabbix, foi utilizada a instalação via pacotes e seguido de acordo com a documentação

oficial do Zabbix. A integração com a ferramenta Grafana alcançou-se por meio da utilização do Zabbix plugin, disponibilizado pelo próprio site do Grafana.

Posteriormente com o Zabbix já instalado é efetuado o cadastramento dos *hosts* que serão monitorados, juntamente com a associação a seus devidos grupos e *templates*. Com as configurações iniciais efetivadas, foram então programadas ações automáticas para eventos como: restabelecimento de serviços do apache, SSH, e Agente Zabbix. Para que seja possível a atuação direta do Zabbix na solução de falhas reportadas pelo monitoramento, foi necessário habilitar o Agente Zabbix para que executasse comandos remotos nos *hosts* monitorados.

A interação dos alertas e eventos gerados pelo sistema, apresentam-se configurados através do painel principal da ferramenta, *dashboards* presentes no Grafana e no Telegram. De modo a garantir diversos meios de visualização e interação com o usuário.

4.2. Planejamento

Nesta fase, será apresentado o planejamento para o desenvolvimento do sistema, baseado no levantamento dos requisitos funcionais e requisitos não funcionais, bem como no cenário de aplicação (APÊNDICE A). O desenvolvimento foi constituído pela implementação dos *scripts* e *templates* e suas configurações. A integração da ferramenta Grafana fez parte essencial do sistema, contribuindo com a visualização das métricas implementadas. Posteriormente, os *scripts* e *templates* desenvolvidos foram importados ao sistema de forma a complementá-lo como novas funcionalidade.

Na Tabela 1, são listados os requisitos funcionais (RF), os quais especificam as funções e comportamentos do sistema.

Tabela 1. Requisitos funcionais (RF)

ID	Descrição	Relevância	Complexidade
RF01	O sistema deverá monitorar todas as impressoras conectadas na rede, fazendo uso de <i>templates</i> para monitorar serviços, como nível de toner, quantidade de impressões e status dos cilindros.	Essencial	Baixa
RF02	O sistema deverá exibir alertas, classificando o grau de severidade da falha, e notificar os usuários, fazendo uso de <i>scripts</i> para integrar com outros serviços.	Essencial	Baixa
RF03	O sistema deverá monitorar itens e aplicações dos <i>hosts</i> , utilizando <i>scripts</i> para buscar informações e associar à aplicação que deverá ser monitorada.	Essencial	Baixa
RF04	O sistema deverá ter ações automatizadas para determinados eventos detectados, como o restabelecimento dos serviços SSH, apache e agente Zabbix, após sua queda.	Desejável	Baixa

RF05	O sistema deverá fazer uma busca nas informações coletadas, gerando representações gráficas e relatórios para o usuário.	Essencial	Baixa
-------------	--	-----------	-------

Dando continuidade, na Tabela 2, foram descritos os requisitos não funcionais (RNF), essenciais para o desenvolvimento do sistema.

Tabela 2. Requisitos não funcionais (RNF)

ID	Descrição	Relevância	Complexidade
RNF01	Os <i>scripts</i> serão desenvolvidos através da linguagem Shell Script	Essencial	Média
RNF02	A ferramenta Zabbix deverá ser instalada no sistema operacional CentOS 8.	Essencial	Baixa
RNF03	O sistema será implantado em máquinas virtuais.	Essencial	Baixa
RNF04	O sistema fará o uso da ferramenta Grafana integrado ao ambiente Zabbix.	Essencial	Baixa

4.3. Fluxo de execução do sistema

Nesta seção, será apresentado o fluxo de execução do sistema diante de adversidade encontrada na rede e, então, realizada uma comparação com o fluxo atual usado na prefeitura.

Como à prefeitura, não possuía um sistema de monitoramento de rede, os problemas que ocasionalmente acontecem são tratados de forma empírica e grande parte das falhas detectadas são relatadas por terceiros, quando já se encontram em estágio avançado (APÊNDICE B).

A Figura 7 retrata o fluxo de atividades para resolução de falhas, porém otimizados com a aplicação do Zabbix. Nesta figura, é observada uma mudança significativa nas tarefas, dado que terá apenas duas tarefas de usuário e o restante automatizado pelo sistema.

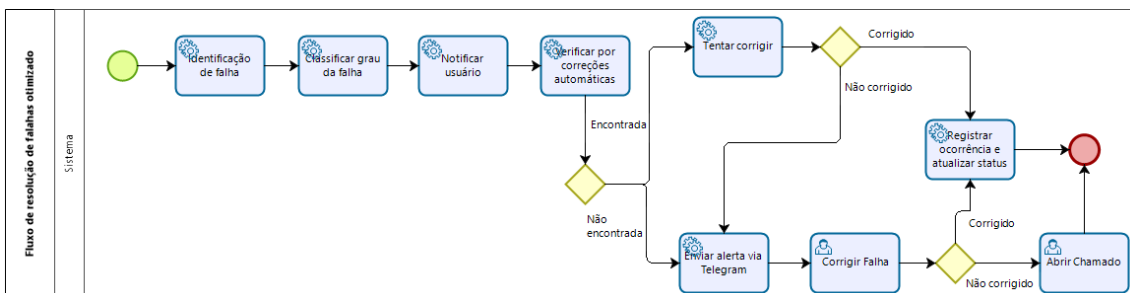


Figura 7. Fluxo de resolução de falhas otimizado

As tarefas otimizadas são acionadas quando um *trigger* é disparado, em seguida é classificado o grau de severidade. Posteriormente, é notificada a falha no painel de monitoramento e verificada por ações pré-configuradas, levando em conta o grau da falha. As falhas não corrigidas ou que detenham um grau elevado de severidade, geram alertas imediatamente ao usuário, sendo enviados pelo Telegram.

Todas essas ações, eventos e *triggers* fornecem a possibilidade de utilização de *scripts* e *templates*, para complementar funções que não são encontradas nativamente na ferramenta.

4.4. Implementação

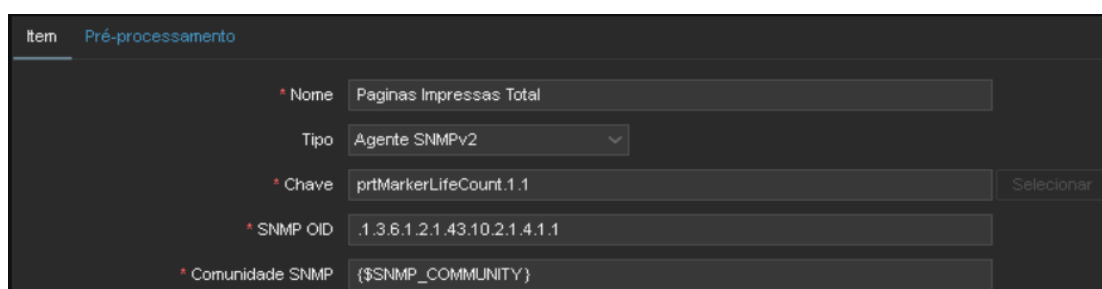
Para a concepção desta fase foram implementados *scrips* e *templates* com intuito de adequar a ferramenta de monitoramento com as necessidades específicas do ambiente de rede da prefeitura.

Na implementação dos *templates*, foi utilizado o comando `#snmpwalk -v 2c -c public "ip do host"`, que permite coletar informações de qualquer dispositivo que tenha implementado em seu sistema o protocolo SNMP. Mediante a esses dados foi possível identificar o SNMP OID, neste caso referente ao contador de páginas impressas. E então é realizado o cadastramento do item que fará a coleta. A Figura 8 demonstra a execução do comando citado anteriormente, onde a linha destacada representa o OID relacionando ao contador de impressões.

```
SNMPv2-SMI::mib-2.43.10.2.1.10.1.1 = INTEGER: 2400
SNMPv2-SMI::mib-2.43.10.2.1.11.1.1 = INTEGER: 4233
SNMPv2-SMI::mib-2.43.10.2.1.12.1.1 = INTEGER: 4233
SNMPv2-SMI::mib-2.43.10.2.1.13.1.1 = INTEGER: 4233
SNMPv2-SMI::mib-2.43.10.2.1.14.1.1 = INTEGER: 4233
SNMPv2-SMI::mib-2.43.10.2.1.15.1.1 = INTEGER: 0
SNMPv2-SMI::mib-2.43.11.1.1.2.1.1 = INTEGER: 1
```

Figura 8. Execução do comando *snmpwalk*.

A Figura 9 exibe a etapa de cadastramento do novo item que será monitorado, assim como, a chave aplicada para a construção das médias de folhas impressas por dia, semana e mês.



Item	Pré-processamento	
* Nome	Paginas Impressas Total	
Tipo	Agente SNMPv2	
* Chave	prtMarkerLifeCount.1.1	Selecionar
* SNMP OID	.1.3.6.1.2.1.43.10.2.1.4.1.1	
* Comunidade SNMP	{\${SNMP_COMMUNITY}}	

Figura 9. Cadastro de itens em um *template*.

Após o cadastro de itens no Zabbix foram elaboradas *triggers* para execução de comandos remotos, geração de alertas e notificações. Para a o desenvolvimento das *triggers* é implementado expressões que atuam comparando os valores recebidos do agente até que um valor definido seja atingido. Na Figura 10 é apresentada a construção de uma *trigger* que alerta o usuário quando o nível do toner de alguma impressora for menor que 10%.

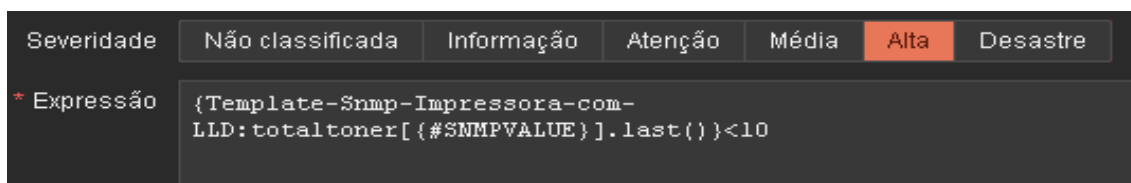


Figura 10. *Trigger* relacionada ao nível de toner.

Também se adequou as mídias que vão enviar os alertas, notificando o usuário sobre as falhas encontradas na rede e seu grau de severidade (APÊNDICE B). Para o envio das notificações dos alertas gerados, foi consumido a mídia padrão para o envio de e-mails, e implementado a integração com o Telegram. Com este serviço possibilitou a criação de um *bot*, um robô que automatiza o encaminhamento das mensagens de alertas.

Para proceder com a integração do Telegram foi preciso importar um *template*, disponibilizado no fórum oficial do Zabbix, e passado as informações referentes ao *Token* e *ID* do *bot* gerado. Essas informações são obtidas após a criação do *bot* diretamente na plataforma Telegram, por meio do comando `#!/newbot`.

Com as configurações dos *templates* concluídas, procedeu-se com a elaboração das ações e comandos remotos executados para o restabelecimento de serviços essenciais os servidores. Inicialmente para que ações pudessem ser tomadas automaticamente, foi preciso criar um usuário e dar permissões a ele, para que o Zabbix conseguisse executar comandos no modo de super usuário. Subsequentemente é implementado no Zabbix o *script* que virá a ser efetivado quando a *trigger* que foi associada a ele for ativada. A Figura 11 expõe como fica estabelecido o *host*, e qual servidor que será executado o *script*.

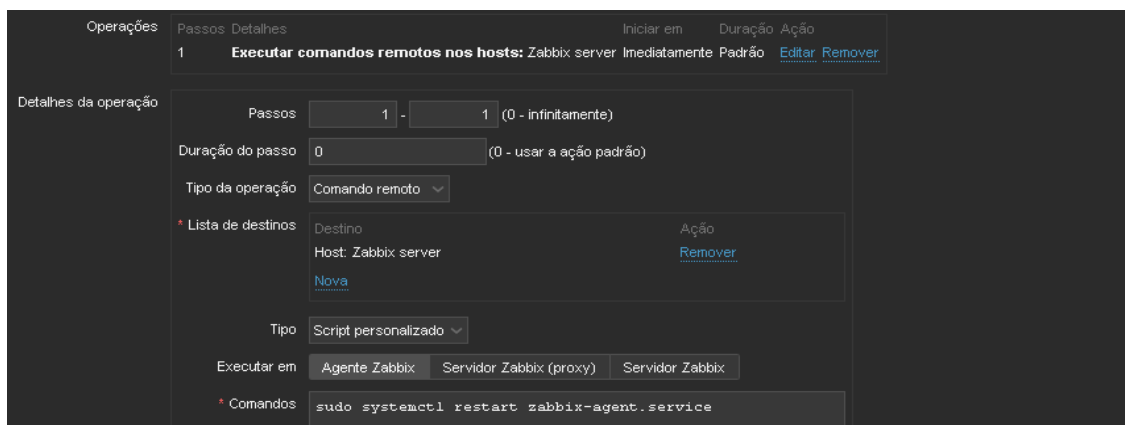


Figura 11. Execução de comando remoto para reiniciar o serviço do Zabbix Agent.

4.5. Teste de desempenho e implantação

Para realizar o teste de desempenho, foi utilizada a ferramenta iPerf3, que mediu o tráfego de rede de um determinado ponto a outro da rede, a variação e perda de pacotes, largura de banda e ainda suportando a alteração entre os protocolos UDP (*User Datagram Protocol*) e TCP (*Transmission Control Protocol*) para a transmissão dos pacotes.

Para proceder com os testes, foram empregados dois computadores localizados em diferentes pontos da rede, atribuindo um deles como servidor e o outro como cliente.

Esses testes foram aplicados diversas vezes até que se obtivesse os dados de cada *switch* da rede.

Os testes resultaram na avaliação de seis *switches*, dispostos no setor de informática, setor de telefonia, setor de fiscalização e setor de agricultura. A banda avaliada foi limitada a 100Mb/s pois apenas o *switch* principal possui portas giga. Com os testes encontrou-se perdas graves no link entre o *switch* do setor de telefonia para o da agricultura. Conforme na Figura 12, foi executado o comando #iperf -c “ip do servidor” -d -b 100M -u, que identificou a ocorrência de até 89% de perdas no tráfego de download, apesar da banda atingir os 100 Mb/s disponíveis.

```
[ ID] Interval          Transfer      Bandwidth    Jitter      Lost/Total Datagrams
[  4]  0.00-10.00 sec   119 MBytes   100 Mbits/sec  0.828 ms   13643/15251 (89%)
[  4] Sent 15251 datagrams

iperf Done.
```

Figura 13. Teste de download em UDP, no *switch* da telefonista.

Após a conclusão destes testes, foi analisado a média geral do tráfego de upload e download entre todos os *switches*, e obteve-se respectivamente 90.7 Mb/s e 93.5 Mb/s, desconsideram o link entre os setores de telefonia e agricultura, alcançou-se uma taxa de perdas inferior a 1%.

Na implantação não houve dificuldades, as instalações e configurações do ambiente procederam-se como o planejado e com total apoio da prefeitura, apenas foi alterado a quantidade de máquinas virtualizadas, pois não houve a necessidade de separar o servidor Zabbix do agente Zabbix. A instalação do servidor foi mantida utilizado um computador do departamento de TI com as configurações de: 8 Gb de RAM, processador Intel Core i5-3470, SSD de 240 Gb e HD de 500 Gb.

6. Resultados e Discussões

A construção deste trabalho resultou em um ambiente de monitoramento de rede, e nos testes dos links entre os *switches* da prefeitura de São Sepé.

Após o desenvolvimento e a certificação que todo ambiente de rede estava sendo monitorado, apresentou-se a ferramenta Zabbix para o responsável pelo setor de TI da prefeitura. Junto a ele, foram elaborados demonstrações e testes da ferramenta para os usuários, os quais resultaram em feedbacks positivos. Segundo o responsável pelo setor de TI é de extrema importância se ter um controle e o monitoramento dos eventos que ocorrem na rede, para melhor poder gerenciá-los e planejar *upgrades* futuros. Inclusive ressaltou os benefícios que a ferramenta proporcionou a prefeitura no quesito da gestão efetiva da troca e obtenção dos suplementos das impressoras.

Esta proposta foi apresentada no SEPE (Simpósio de Ensino, Pesquisa e Extensão) no ano de 2020 na instituição UFN (Universidade Franciscana). Esta oportunidade foi bem importante para expor a ideia do trabalho, esclarecer dúvidas sobre o tema proposto, além dos feedbacks que ajudaram no enriquecimento do trabalho.

A respeito da aplicação, na Figura 13 é exposto as *dashboards* no Grafana, que faz a apresentação dos dados coletados para o usuário final.

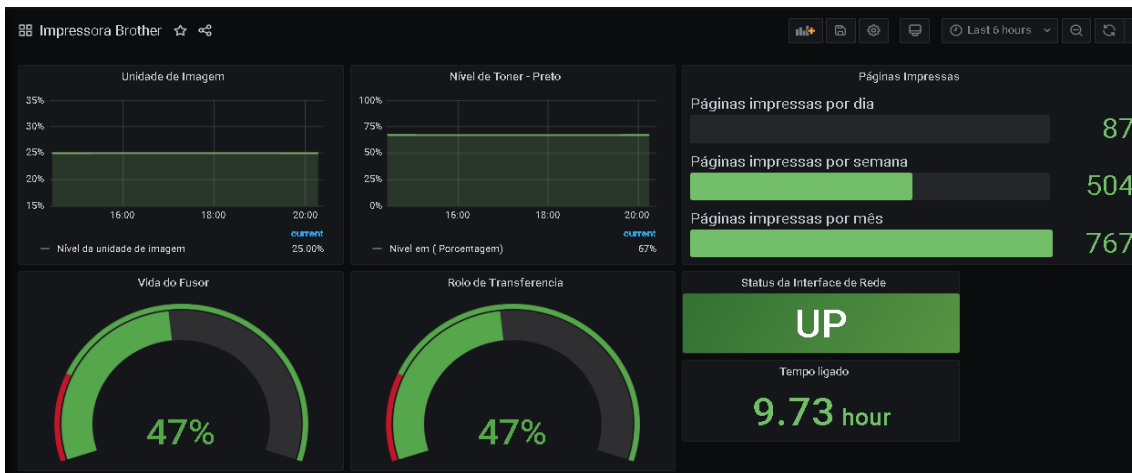


Figura 13. *Dashboard* com informações obtidas de uma impressora.

A Figura 14 mostra os alertas estruturados no Grafana, que também são disponibilizados por meio das mensagens enviadas do Telegram.

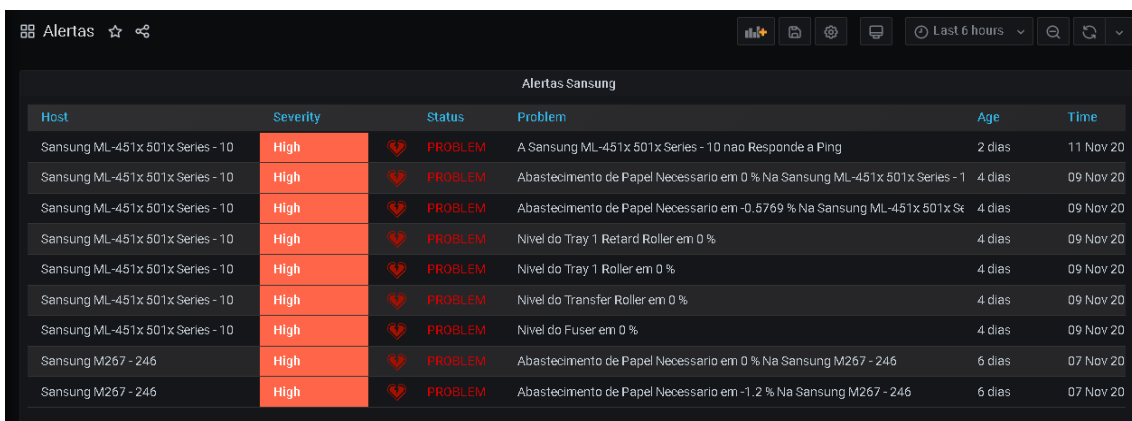


Figura 14. *Dashboard* de alertas das impressoras Samsung.

E subsequentemente é ilustrado na Figura 15 as notificações enviadas pelo *bot* Zabbix_Prefeitura, indicando a falha encontrada, como também o período de sua ocorrência e restabelecimento.

ZP Zabbix_Prefeitura

Problem: Nivel do Black Toner S/N :CRUM-14050394825 em 9 % 08:57:24
 Problem started at 06:57:05 on 2020.12.16
 Problem name: Nivel do Black Toner S/N :CRUM-14050394825 em 9 %
 Host: Samsung M267 - 246
 Severity: High

Resolved: Nivel do Black Toner S/N :CRUM-14050394825 em 9 % 09:57:23
 Problem has been resolved at 07:57:05 on 2020.12.16
 Problem name: Nivel do Black Toner S/N :CRUM-14050394825 em 9 %
 Host: Samsung M267 - 246
 Severity: High

Original problem ID: 150427

Figura 15. Notificação recebida no Telegram, após o nível do toner atingir menos de 10%.

6. Conclusão

O presente trabalho apresentou a proposta de implantação de um sistema de monitoramento de rede para a Prefeitura Municipal de São Sepé - RS. Com o estudo realizado na instituição, foi buscado por meio da utilização da ferramenta de monitoramento Zabbix, trazer uma solução *open source* que aprimoraria o gerenciamento da rede como também as atividades desempenhadas pelo setor de TI.

Os trabalhos correlatos foram essenciais para a elaboração desta proposta, visto que serviram como base para a escolha e utilização da ferramenta mais adequada para o ambiente de rede da prefeitura.

O sistema de monitoramento implantado possibilitou uma grande melhoria na rede aplicada da prefeitura, melhorando a gestão do ambiente e otimizando tarefas que eram efetuadas manualmente. A integração com a ferramenta Grafana e Telegram, foram partes essenciais deste trabalho, pois com eles alcançou-se uma melhor interação com o usuário, possibilitando uma visão mais agradável das informações monitoradas e flexibilizado o recebimento dos alertas. No decorrer dos testes de performance, pôde-se ter uma percepção geral do desempenho da rede, como também na identificação de perdas no tráfego interno.

Diante disso, observaram-se trabalhos futuros que poderão ser desenvolvidos para aprimorar ainda mais o monitoramento da rede e abranger outras secretarias que se encontram fora do prédio principal da prefeitura. Para isso é sugerido a implantação do Zabbix proxy, que faria remotamente a coleta dos dados, usufruindo da API do Zabbix para o desenvolvimento de uma aplicação que gerencie relatório de monitoramento em alto nível.

Referências

- Alvarenga, R. P. C. (2015) “Monitoramento e segurança: uma abordagem sobre como o Zabbix pode contribuir com relação à segurança e a gestão de suas melhores práticas em Tecnologia da Informação”, <http://encurtador.com.br/gks07>, Março.
- Andreoli, Y. (2016) “Análise comparativa entre ferramentas para gerenciamento e monitoramento de redes”, <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/7301>, Março.
- Bahls, A. (2016) “Monitoramento proativo do ambiente de rede utilizando o software Zabbix”, <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/7417>, Abril.
- Black, T. (2008) “Comparação de Ferramentas de Gerenciamento de Redes”, <https://lume.ufrgs.br/handle/10183/15986>, Maio.
- Campos, E. (2018) “Estudo de caso de ferramentas para o Gerenciamento de Rede de Computadores”, <https://repositorio.ifsc.edu.br/handle/123456789/345>, Abril.
- Figueiredo, Ê. (2016) “Prontuário Eletrônico x Infraestrutura de TI x Cidade Digital”, <https://redestecnologia.com.br/prontuario-eletronico/>, Maio.

- Gomes, P. (2017) “Entenda o que é o protocolo SNMP e sua importância no monitoramento”, <https://www.opservices.com.br/snmp/>, Abril.
- Gomes, P. (2019) “O que é e como funciona o Grafana? Entenda aqui”, <https://www.opservices.com.br/grafana/>, Maio.
- iPerf. (2020) “iPerf - The ultimate speed test tool for TCP, UDP and SCTP”, <https://iperf.fr/>, Maio.
- Lima, J. R. (2014) “Monitoramento de Redes com Zabbix”, Brasport, Rio de Janeiro.
- Lousada, F. (2015) “Introdução ao Shell Script no Linux”, <https://www.devmedia.com.br/introducao-ao-shell-script-no-linux/25778>, Abril.
- Maldonado, R. (2016) “Monitoramento de Rede Utilizando Zabbix”, http://zabbixbrasil.org/files/Monografia_Fatec_Mococa_Zabbix-Rodrigo_Maldonado.pdf, Abril.
- Muxfeldt, P. (2017) “Linux o Shell”, <https://www.devmedia.com.br/introducao-ao-shell-script-no-linux/25778>, Abril.
- Pinheiro, J. M. (2002) “Gerenciamento de Redes de Computadores”, <http://www.allnetcom.com.br/upload/GerenciamentodeRedes.pdf>, Abril.
- Rocha, R. (2020) “O Telegram como ferramenta estratégica para o seu negócio”, <https://www.ecommercebrasil.com.br/artigos/o-telegram-como-ferramenta-estrategica-para-o-seu-negocio/>, dezembro.
- Silva, W. M. C., Medeiros, R. M. e Martins, R. S. (2015) “Análise e gerenciamento de rede usando uma metodologia proativa com Zabbix”, <http://zabbixbrasil.org/files/2441-11176-1-PB.pdf>, Maio.
- Zabbix SIA. (2020) “Zabbix Documentation 4.4”, <https://www.zabbix.com/documentation/current/pt/manual/concepts/proxy>, Abril.

Apêndice A. Diagrama de caso de uso

Na Figura 5, é apresentado o diagrama de casos de uso, responsável por descrever as novas funcionalidades adicionadas no sistema somado com as interações dos usuários que a executam.

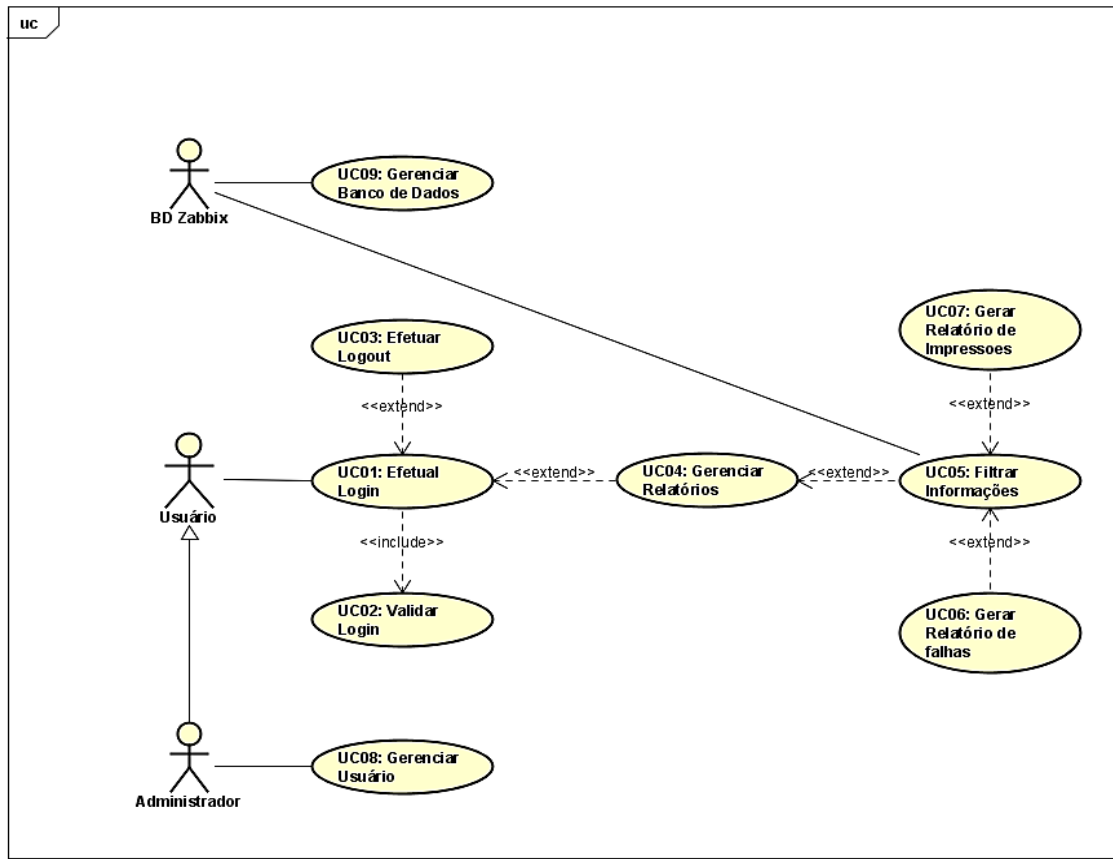


Figura 5. Diagrama de casos de uso.

Apêndice B. Classificação de severidade das *triggers*

Na Figura 6, está representado o fluxo conforme são tratadas as falhas na rede.

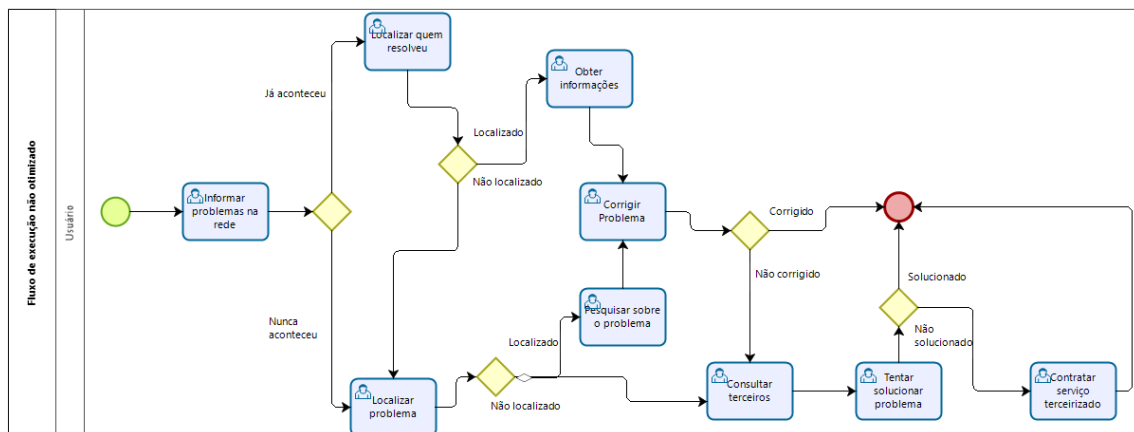


Figura 6. Fluxo de resolução de falhas atual

Apêndice C. Classificação de severidade das *triggers*

SEVERIDADE	DEFINIÇÃO	COR
Não classificado	Severidade desconhecida.	Cinza
Informação	Apenas informacional.	Verde claro
Atenção	Esteja avisado.	Amarelo
Média	Problema (incidente) médio.	Laranja
Alta	Algo importante ocorreu.	Vermelho
Desastre	Desastre. Perdas financeiras, perda total de capacidade etc.	Vermelho escuro

Tabela 3. Níveis de severidade das *triggers* encontradas no Zabbix [Zabbix SIA 2020].