UNIVERSIDADE DO SUL DE SANTA CATARINA

ANDRÉ LUIZ MARIANO DO VALE

MONITORAMENTO DE REDES:

A IMPORTÂNCIA DO MONITORAMENTO DE REDES PARA A SEGURANÇA DA INFORMAÇÃO

Palhoça

2017

ANDRÉ LUIZ MARIANO DO VALE

MONITORAMENTO DE REDES:

A IMPORTÂNCIA DO MONITORAMENTO DE REDES PARA A SEGURANÇA DA INFORMAÇÃO

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação,** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientador: Prof. Nilce Miranda Ayres

Palhoça

2017

ANDRÉ LUIZ MARIANO DO VALE

MONITORAMENTO DE REDES:

A IMPORTÂNCIA DO MONITORAMENTO DE REDES PARA A SEGURANÇA DA INFORMAÇÃO

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Palhoça, 15 de outubro de 2017.

Prof. e orientador Nilce Miranda Ayres, Me.
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Em primeiro lugar, e sempre, agradeço a Deus pela vida e pela qualidade de vida que me permite ter. Agraço muito a minha amada mãe, por todos os esforços e cuidados que sempre teve comigo. Também um agradecimento especial ao meu pai, por sua grande determinação e dedicação ao trabalho, durante toda sua vida, para proporcionar uma vida digna à família. Não está mais entre nós fisicamente, mas estará sempre em minha memória. Agradeço também a todos os colaboradores da Unisul, pela dedicação e atenção que nos concedem sempre que precisamos. E quando pensamos em contribuição à humanidade através do desenvolvimento de softwares não posso deixar de agradecer as grandes contribuições de Richard Stallman pelo Projeto GNU, ao Linus Torvalds pelo Linux e ao Alexei Vladishev pelo Zabbix.

RESUMO

Este trabalho tem a finalidade de identificar, através de uma análise de uma versão do software instalada em laboratório, se a utilização de um software gratuito e de código aberto, como o Zabbix por exemplo, pode contribuir com a segurança da informação das organizações. Este estudo de caso utiliza uma pesquisa explicativa.

Palavras-chave: Monitoramento. Redes de computadores. Código aberto. Open Source. Segurança da Informação. Zabbix.

Lista de figuras

Lista de tabelas

Sumário

1 INTRODUÇÃO

A segurança da informação se mostra cada vez mais necessária nas empresas, visto que a informação se tornou um ativo de grande valor. As ferramentas de monitoramento tem um potencial muito grande para contribuir com a continuidade do negócio das empresas. Os softwares proprietários de monitoramento possuem um elevado custo de licenciamento, portanto este estudo foi elaborado para verificar, ainda que em um ambiente de laboratório, se um software de código aberto, sem custo de licenciamento, reúne recursos, qualidade e características que podem atender aos objetivos, como uma alternativa mais econômica, para contribuir com a segurança da informação das empresas.

Este trabalho está estruturado da seguinte forma: inicia-se com o tema do trabalho, em seguida apresento os objetivos a serem alcançados e os procedimentos metodológicos utilizados, faço uma apresentação e uma análise da realidade observada, depois apresento uma proposta de solução da situação-problema, faço minhas considerações finais e por fim, temos uma lista das referências bibliográficas.

2 TEMA

Existem muitas variáveis que podem causar a indisponibilidade de serviços de TI nas organizações, comprometendo a segurança da informação. Segundo Gonçalves (2000), “se não existissem preocupações com risco de segurança relativos à conectividade na Internet, não haveria necessidade de firewalls e nem de outros mecanismos de defesa”. Os níveis de utilização dos recursos computacionais precisam ser acompanhados e monitorados constantemente para verificar se estão dentro das condições normais e necessárias para o correto funcionamento dos sistemas. Diversos eventos, dos mais variados tipos, podem ocorrer em uma rede a qualquer momento. Estes eventos precisam ser analisados e classificados para identificar se podem ou não representar algum risco à segurança da informação. De acordo com Horst; Pires e Déo (2015, p. 19), “Zabbix é uma ferramenta moderna, Open Source e multiplataforma, livre de custos de licenciamento, pois sua licença é a GPLv2 (*GNU General Public License*). Tem apenas uma versão, que é considerada de classe Enterprise, sendo utilizada para monitorar a disponibilidade e o desempenho de aplicações, ativos e serviços de rede por todo o mundo.”.

A justificativa para a realização deste estudo, se dá em função da necessidade que as organizações tem de manter um nível mínimo aceitável da segurança da informação e do alto custo com licenciamento de softwares proprietários, que tem como função o monitoramento de ativos e serviços de rede. Portanto, por uma questão de economia, muitas empresas precisam encontrar ferramentas maduras, mas que sejam de código aberto, para ajudá-las nesta função. Como atuo na área de administração de servidores, também senti a necessidade de utilizar ferramentas de monitoramento e percebi o grande valor que elas podem agregar ao negócio das empresas. Quando conheci o Zabbix fiquei muito impressionado com a quantidade de recursos disponíveis e com a excelente qualidade que apresenta, despertando em mim um desejo de conhecer e explorar cada vez mais seu potencial e identificar uma boa oportunidade para trabalhar com esta ferramenta, oferecendo um serviço que permite aumentar a disponibilidade dos recursos de rede das empresas.

A partir do contexto apresentado, este trabalho pretende responder a seguinte questão: sistemas de monitoramento de código aberto podem contribuir com a segurança da informação nas organizações?

3 OBJETIVOS

3.1 OBJETIVO GERAL

Identificar se o monitoramento de ativos e serviços de infraestrutura de rede, realizado com o Zabbix, que é um software gratuito e de código aberto, pode contribuir com a segurança da informação das organizações.

3.2 OBJETIVOS ESPECÍFICOS

- Verificar se o Zabbix é capaz de monitorar a disponibilidade de dispositivos e serviços de rede.
- Verificar se o Zabbix é capaz de gerar alertas de incidentes causados pela indisponibilidade de algum dispositivo ou serviço de rede.
- Verificar se a utilização do Zabbix pode contribuir para reduzir o *downtime* (tempo de parada não programada) de serviços de rede.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

Através de uma pesquisa do tipo explicativa, será utilizado como campo de estudo o software gratuito e de código aberto, Zabbix, para a realização deste estudo de caso. Este software tem a capacidade de, além de outras coisas, efetuar monitoramento de dispositivos e serviços de redes, bem como registrar os dados do monitoramento automaticamente em um banco de dados. Quando necessário é possível exibir estes dados na forma de relatórios e de gráficos, além de possuir a capacidade de transformar os dados em informações de acordo com as definições e configurações realizadas pelo administrador do sistema.

Por ser uma pesquisa do tipo explicativa “este tipo de pesquisa preocupa-se em identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos.” (GIL, 2007 apud UFRGS, 2009, p. 35).

4.2 INSTRUMENTOS DE COLETA DE DADOS

Os instrumentos de coleta de dados adotados neste trabalho são descritos na tabela 1.

Tabela 1: Instrumento de coleta de dados

Instrumento de coleta de dados	**Universo pesquisado**	**Finalidade do Instrumento**
Observação direta ou dos participantes	A observação será feita em um laboratório, com o software Zabbix instalado.	Efetuar o monitoramento em um ambiente de laboratório, conhecer os recursos de monitoramento oferecidos pelo software e visualizar os dados apresentados.
Documentos	Será utilizado como referência bibliográfica o livro De A a ZABBIX, publicado pela Novatec de autoria de: Adail Spínola, Aécio dos Santos e André Déo.	Buscar orientações sobre o funcionamento do software, como operá-lo e configurá-lo, bem como conhecer seus recursos.
Dados arquivados	Os dados coletados através do monitoramento são armazenados em banco de dados MySQL, por exemplo, e apresentados em uma interface web pelo Zabbix.	Demonstrar como os dados são apresentados para o analista de monitoramento.

Fonte: Do Autor.

5 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

5.1 SOBRE A SOLUÇÃO OPEN SOURCE DE MONITORAMENTO - ZABBIX

O Zabbix é um software de código aberto, idealizado por Alexei Vladishev, quando trabalhava em um grande banco na Letônia, em 1998, e sentiu a necessidade de uma solução de monitoramento. A primeira versão oficial do Zabbix foi lançada em 2001. Desde então, foram lançadas diversas versões, sendo a mais recente a versão 3.4.1, distribuída pela licença GPLv2 GNU *General Public License* (Licença Pública Geral GNU) segunda versão. O Zabbix é considerado pelo Gartner uma das melhores soluções de monitoramento, possui interface traduzida para 25 idiomas. Em 2005, Alexei Vladishev criou a empresa Zabbix SIA responsável por manter o desenvolvimento do software e prestar suporte técnico especializado. Conta com 70 parceiros em diversas partes do mundo (ZABBIX, 2017).

Soluções de monitoramento se tornaram essenciais para muitas organizações, pois a quantidade de dispositivos e serviços de rede aumentou consideravelmente nas últimas décadas, tornando inviável o seu monitoramento manual. Os dispositivos e serviços de rede em uma organização, precisam funcionar 24x7, na grande maioria dos casos, sendo mais um fator a exigir que as organizações implementem soluções de monitoramento automatizado.

Segundo Zabbix (2017), ele tem como objetivo efetuar, de forma automática, o monitoramento de dispositivos, aplicativos e serviços de rede, armazenar os dados em um banco de dados, enviar alertas principalmente via e-mail, SMS e Jabber. Através de sua interface web, também é possível ativar alertas sonoros em caso de incidentes, visualizar painéis de controle, gráficos, mapas e telas com informações de status e performance dos itens monitorados. Mesmo sendo uma ferramenta de código aberto, possui suporte comercial. Um único servidor Zabbix é capaz de fazer o monitoramento de até 25000 hosts.

O Zabbix é uma ferramenta bastante flexível, de classe *enterprise*, capaz de monitorar qualquer coisa. pode ser utilizada em um único servidor, mas também permite que seja implementada em uma estrutura de monitoramento distribuída, coletando informações de diversos locais e concentrando tudo em um único banco de dados. Sua estrutura é composta por diversos sistemas, listados a seguir:

- Zabbix Server - Sistema de monitoramento propriamente dito;

- Zabbix Web - Oferece uma interface com o usuário, por onde é feita sua configuração e administração;
- Zabbix Proxy - É um serviço opcional, mais utilizado em redes remotas realizando um cache dos dados coletados e enviando-os ao servidor central. Também pode ser utilizado para reduzir a carga de processamento do Zabbix Server em redes locais;
- Um banco de dados SQL - Geralmente é utilizado o Mariadb (uma derivação do MySQL) utilizado para armazenar as informações do sistema, como dispositivos a serem monitorados e os dados coletados. Podem ser utilizados outros bancos de dados como PostgreSQL, Oracle, MySQL, SQLite e IBM DB2;
- Zabbix Agent - Pode ser instalado em vários tipos de sistemas operacionais a serem monitorados como Linux, Windows, OS X, entre outros.
- Zabbix Sender - Pode ser utilizado para enviar informações de um host para o servidor Zabbix e
- Zabbix Java Gateway - Pode ser utilizado para coletar um item (dado) através de um contador JMX de aplicações feitas em java.

As informações no Zabbix estão associadas da seguinte forma:

Um host pode ser qualquer nó na rede (servidor, desktop, notebook, impressora, scanner, relógio de ponto, smartphone, tablet, etc.).

Os itens de monitoramento são associados aos hosts de acordo com seus recursos a serem monitorados (ICMP ping, serviços de rede HTTP, ftp, SSH, utilização de disco, carga do sistema, utilização do processador, utilização de memória, tráfego de rede, etc.).

As triggers são associadas aos itens de monitoramento. Elas são configuradas para gerar alertas quando o valor de um item monitorado atingir um nível configurado pelo administrador. Por exemplo, se a utilização de uma unidade de disco atingir 80% da capacidade total, um alerta pode ser gerado informando que o disco está em um nível crítico de utilização. As triggers podem ser criadas e personalizadas de acordo com os níveis aceitáveis de cada item monitorado.

Um gráfico pode conter informações de vários itens monitorados.

Uma tela pode ser criada com vários gráficos a fim de permitir análise do comportamento dos itens monitorados, exibindo seu histórico de acordo com o período selecionado.

Um *slideshow* pode ser criado para alternar a exibição de forma automática das telas cadastradas, permitindo definir quanto tempo, cada tela ficará em exibição.

Descoberta é um recurso muito importante que permite que o Zabbix identifique e cadastre de forma automática os itens encontrados em um host. Se um disco possuir diversas

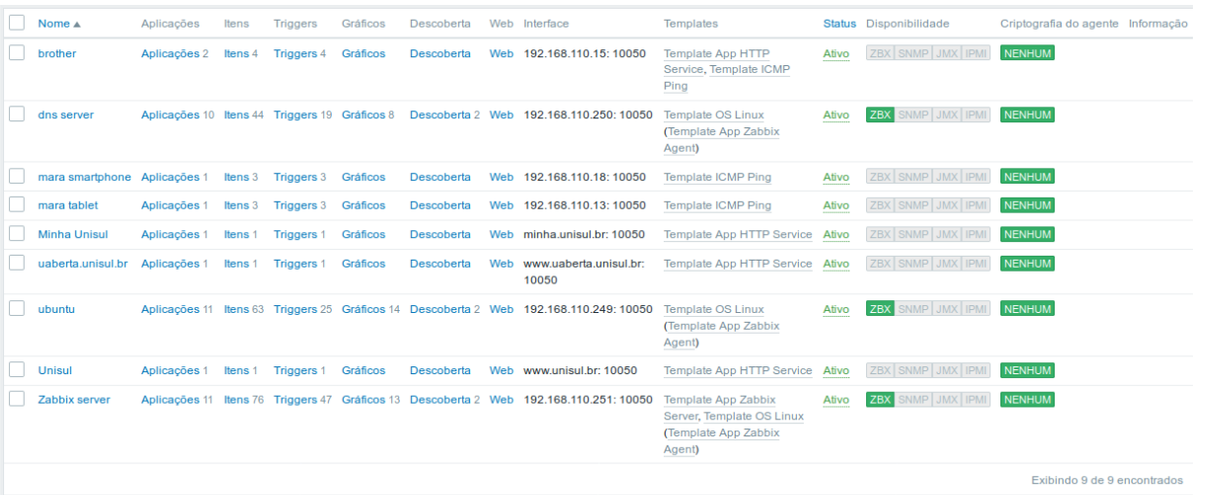
unidades, o Zabbix é capaz de identificar estas unidades e efetuar o monitoramento de cada uma delas de forma automática.

Um *template* pode ser criado com vários itens de monitoramento, triggers, mapas e descoberta.

Os tipos de monitoramento que o Zabbix realiza são: monitoramento simples onde não há nenhuma alteração no host monitorado, monitoramento através da instalação do agente do Zabbix permitindo a coleta de qualquer informação disponível no host e através do protocolo SNMP que pode ser ativado em diversos sistemas operacionais como Linux, OS X, FreeBSD, Windows entre outros, JMX e IPMI.

5.2 DESCRIÇÃO E ANÁLISE DA REALIDADE OBSERVADA

Para o desenvolvimento deste trabalho, foi efetuada a instalação da versão mais recente do Zabbix 3.4.1, para efetuar o monitoramento de dispositivos e serviços em um laboratório, criado na rede doméstica. Os hosts monitorados estão descritos na figura 1, extraída do sistema:



Nome ▲	Aplicações	Itens	Triggers	Gráficos	Descoberta	Web	Interface	Templates	Status	Disponibilidade	Criptografia do agente	Informação
brother	Aplicações 2	Itens 4	Triggers 4	Gráficos	Descoberta	Web	192.168.110.15: 10050	Template App HTTP Service, Template ICMP Ping	Ativo	ZBX SNMP JMX IPMI	NENHUM	
dns server	Aplicações 10	Itens 44	Triggers 19	Gráficos 8	Descoberta 2	Web	192.168.110.250: 10050	Template OS Linux (Template App Zabbix Agent)	Ativo	ZBX SNMP JMX IPMI	NENHUM	
mara smartphone	Aplicações 1	Itens 3	Triggers 3	Gráficos	Descoberta	Web	192.168.110.18: 10050	Template ICMP Ping	Ativo	ZBX SNMP JMX IPMI	NENHUM	
mara tablet	Aplicações 1	Itens 3	Triggers 3	Gráficos	Descoberta	Web	192.168.110.13: 10050	Template ICMP Ping	Ativo	ZBX SNMP JMX IPMI	NENHUM	
Minha Unisul	Aplicações 1	Itens 1	Triggers 1	Gráficos	Descoberta	Web	minha.unisul.br: 10050	Template App HTTP Service	Ativo	ZBX SNMP JMX IPMI	NENHUM	
uaberta.unisul.br	Aplicações 1	Itens 1	Triggers 1	Gráficos	Descoberta	Web	www.uaberta.unisul.br: 10050	Template App HTTP Service	Ativo	ZBX SNMP JMX IPMI	NENHUM	
ubuntu	Aplicações 11	Itens 63	Triggers 25	Gráficos 14	Descoberta 2	Web	192.168.110.249: 10050	Template OS Linux (Template App Zabbix Agent)	Ativo	ZBX SNMP JMX IPMI	NENHUM	
Unisul	Aplicações 1	Itens 1	Triggers 1	Gráficos	Descoberta	Web	www.unisul.br: 10050	Template App HTTP Service	Ativo	ZBX SNMP JMX IPMI	NENHUM	
Zabbix server	Aplicações 11	Itens 76	Triggers 47	Gráficos 13	Descoberta 2	Web	192.168.110.251: 10050	Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Ativo	ZBX SNMP JMX IPMI	NENHUM	

Exibindo 9 de 9 encontrados

Figura 1: Lista de hosts cadastrados a serem monitorados

Fonte: do autor.

Podemos observar que é possível efetuar o monitoramento de hosts na rede local, bem como na Internet, como foi o caso dos três servidores da Unisul. Para os hosts na rede local, o monitoramento é feito via ICMP ping. Nos servidores externos, além do monitoramento de ICMP ping está sendo realizado o monitoramento do serviço web através dos *templates* App HTTP Service. Também foram utilizados os *templates* para OS Linux nos hosts locais criados com o sistema operacional Linux. No servidor DNS foi instalado um agente do Zabbix, permitindo a utilização do *template* App Zabbix Agent, desta forma é o monitoramento de uma quantidade de itens maior, que neste caso são 44 itens. Com relação ao host Zabbix server, também foi possível aplicar o *template* do próprio servidor, que é o App Zabbix Server.

Em seguida destaco algumas telas da interface web do Zabbix, utilizadas pelo administrador do sistema, que permite tanto o cadastro dos *hosts*, *templates*, itens e gatilhos de alertas, como também visualizar o status dos itens monitorados através de relatórios com filtros de pesquisas, mapas e gráficos de histórico.

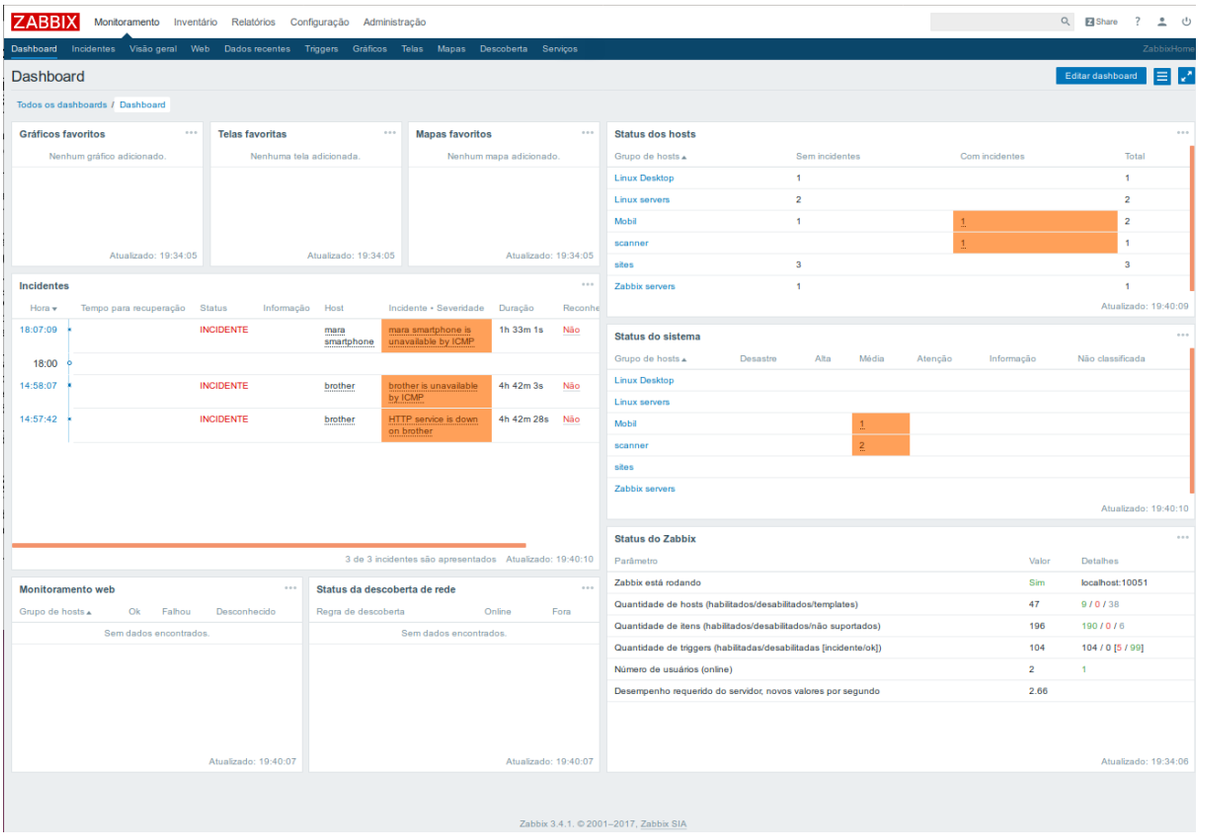


Figura 2: Painel de controle principal

Fonte: do autor.

Na figura 3 podemos ter acesso direto aos incidentes mais recentes. Para uma equipe que trata de incidentes, este é um dos recursos mais importantes da ferramenta, pois ela ajuda na orientação das ações que devem ser tomadas o mais rápido possível para reduzir o tempo de indisponibilidade dos recursos de rede.

Figura 3: Destaque do quadro de alertas de incidentes do painel de controle

Fonte: do autor.

Na figura 4 podemos observar uma tela com o registro do históricos de incidentes registrados automaticamente pelo Zabbix. É um recurso importante que informa a data e a duração de cada incidente. Permite a aplicação dos filtros na parte superior da tela.

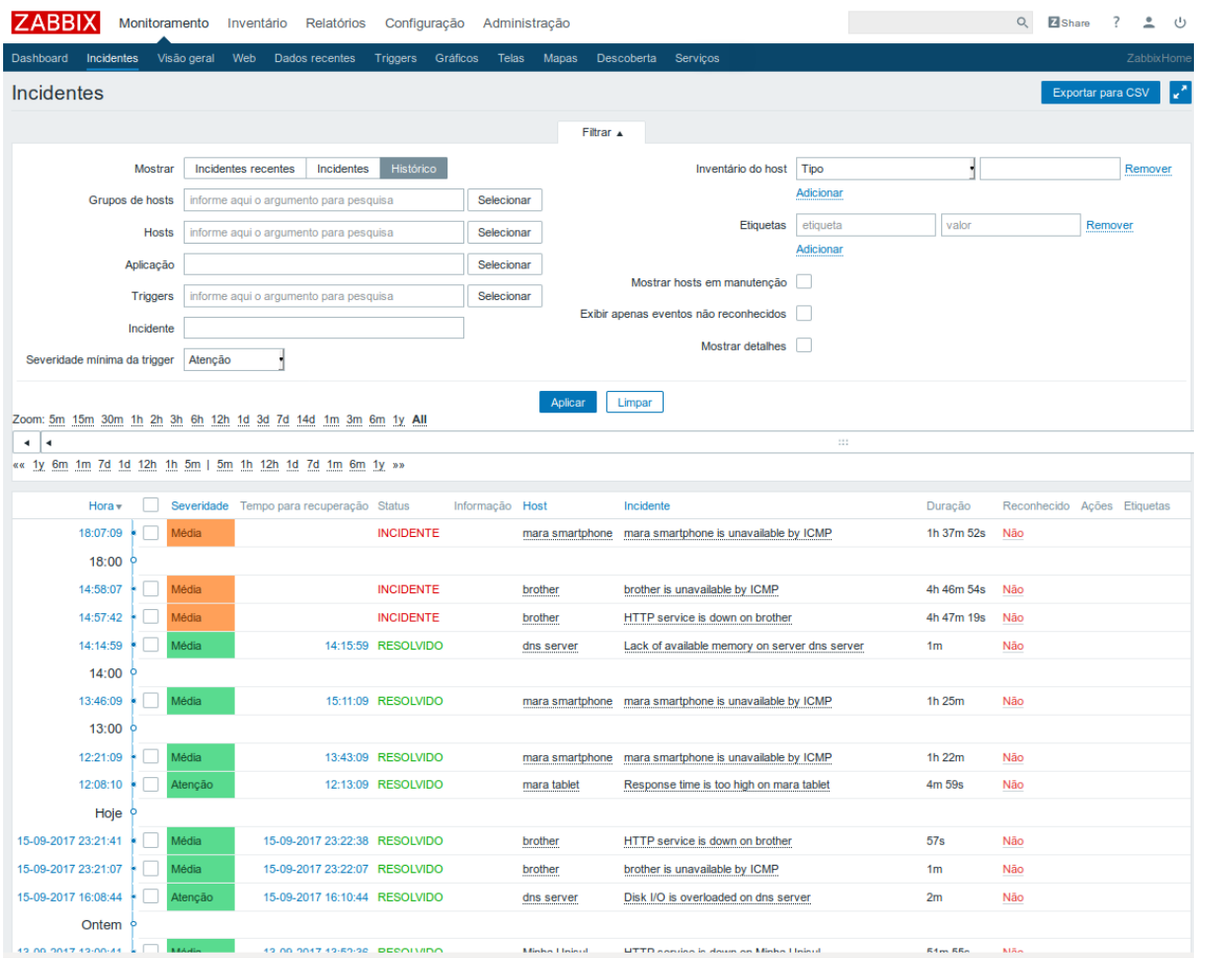


Figura 4: Tela de incidentes detectados pelo Zabbix

Fonte: do autor.

É importante ter uma visão geral do status dos itens monitorados em uma única tela. Este recurso pode ser observado na figura 5. É uma tabela que cruza informações de cada host com os itens monitorados.

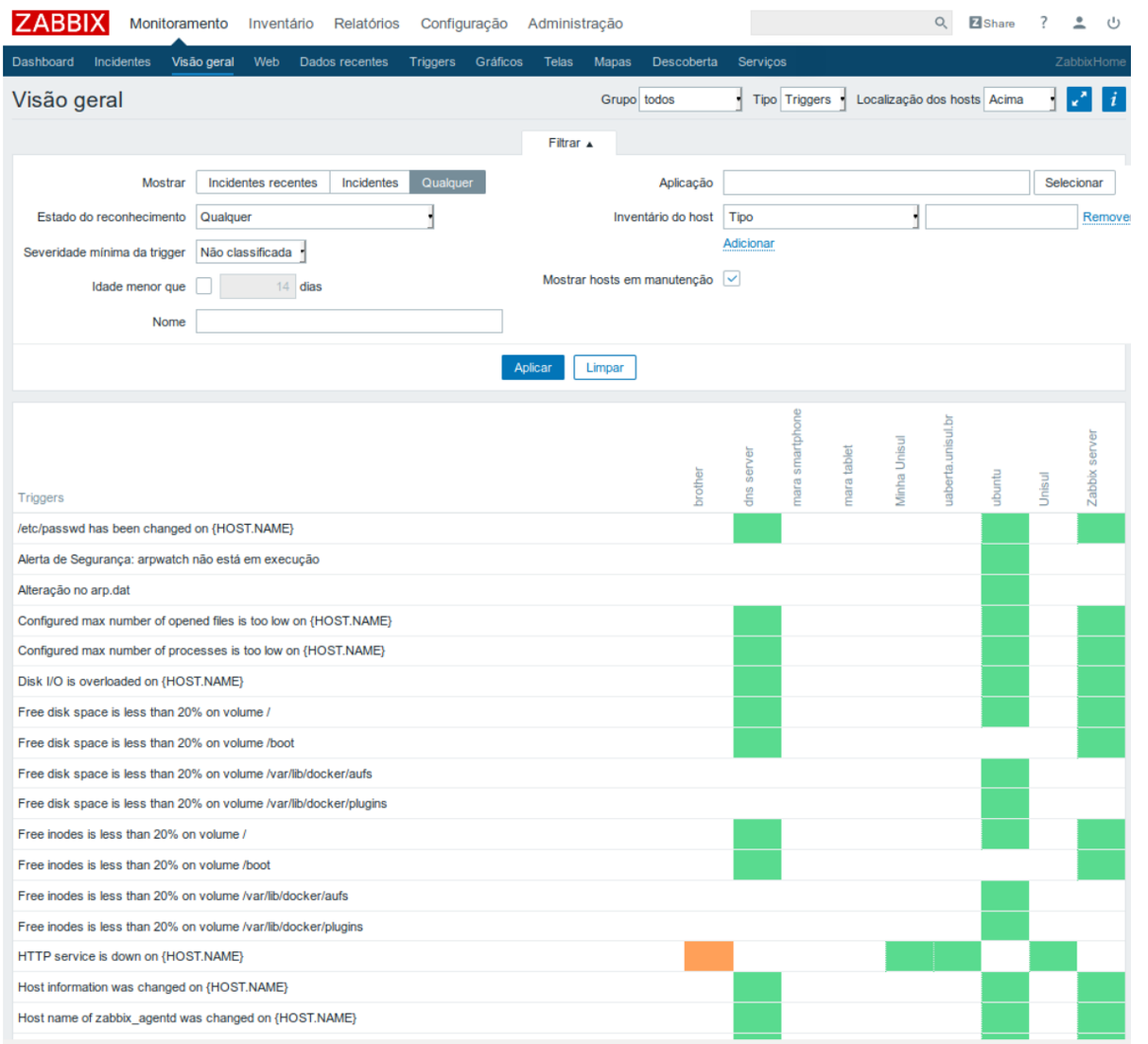


Figura 5: Tela da Visão geral dos dispositivos com o status de seus itens monitorados

Fonte: do autor.

A visualização dos dados através de gráficos é um recurso que permite uma rápida compreensão do comportamento do item monitorado. Na figura 6 temos um gráfico que reúne informações de um determinado item de monitoramento de diferentes hosts. O gráfico possui recursos de navegação podendo avançar o retroceder na linha do tempo, bem como aplicar um zoom em uma região do gráfico para obter maiores de talhes dos dados coletados.

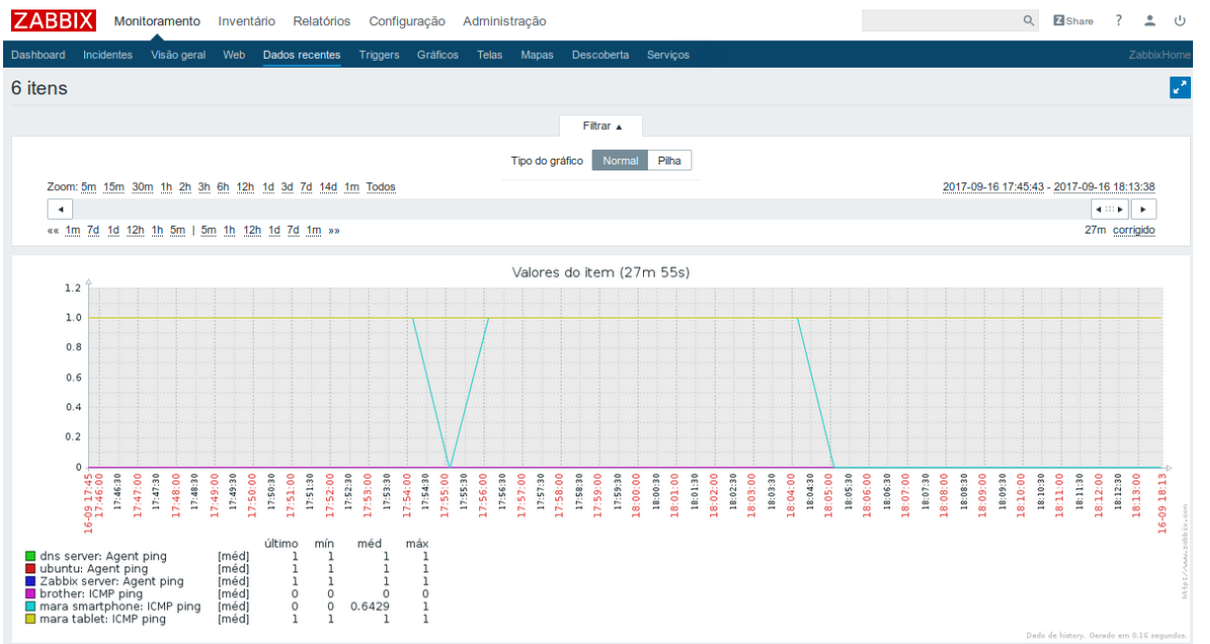


Figura 6: Representação gráfica do status disponibilidade dos hosts locais

Fonte: do autor.

Na figura 7 podemos observar um item monitorado e na legenda o valor de sua trigger. Neste caso o gráfico exibe apenas dois valores, 1 indica disponibilidade, ou seja, seu funcionamento normal e 0 indica indisponibilidade, quando o alerta é emitido.

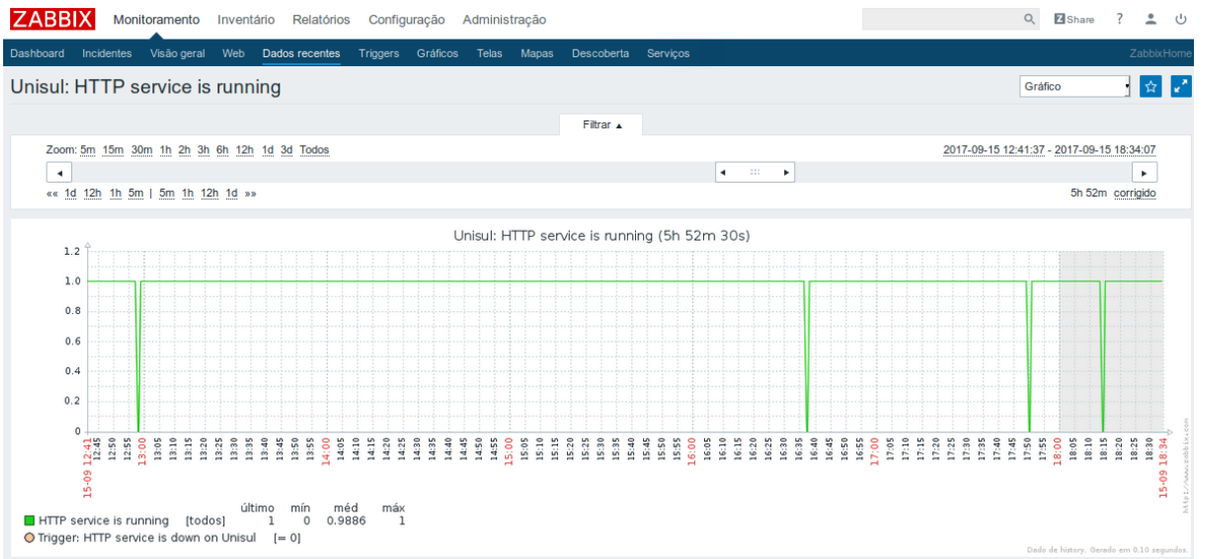


Figura 7: Representação gráfica do status de disponibilidade de um servidor na Internet

Fonte: do autor.

Durante o processo de instalação, o Zabbix já disponibiliza uma grande quantidade de templates que agilizam consideravelmente o tempo de implantação da solução. Os templates podem ser associados manualmente ou automaticamente aos hosts, conforme configuração.

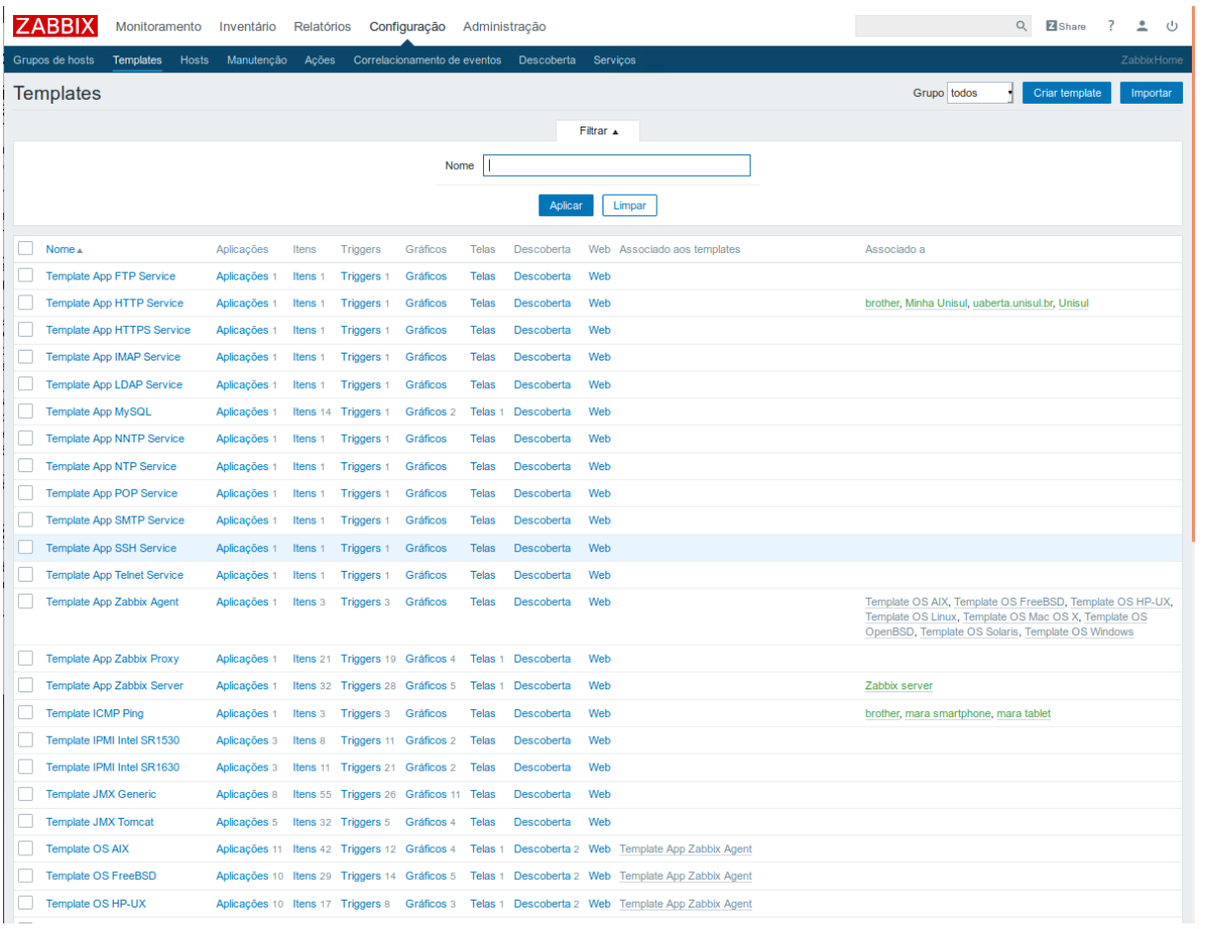


Figura 8: Parte da lista dos templates pré-configurados

Fonte: do autor.

Como pontos fortes do Zabbix podemos destacar que é uma solução bastante robusta, bastante madura em função do seu longo tempo de desenvolvimento, bastante flexível com muitos recursos permitindo personalização de acordo com o ambiente a ser monitorado, como podemos ver na figura 9. É econômico por ser gratuito e de fácil acesso. Há uma declaração da empresa em manter todos os recursos em uma única versão de código aberto.

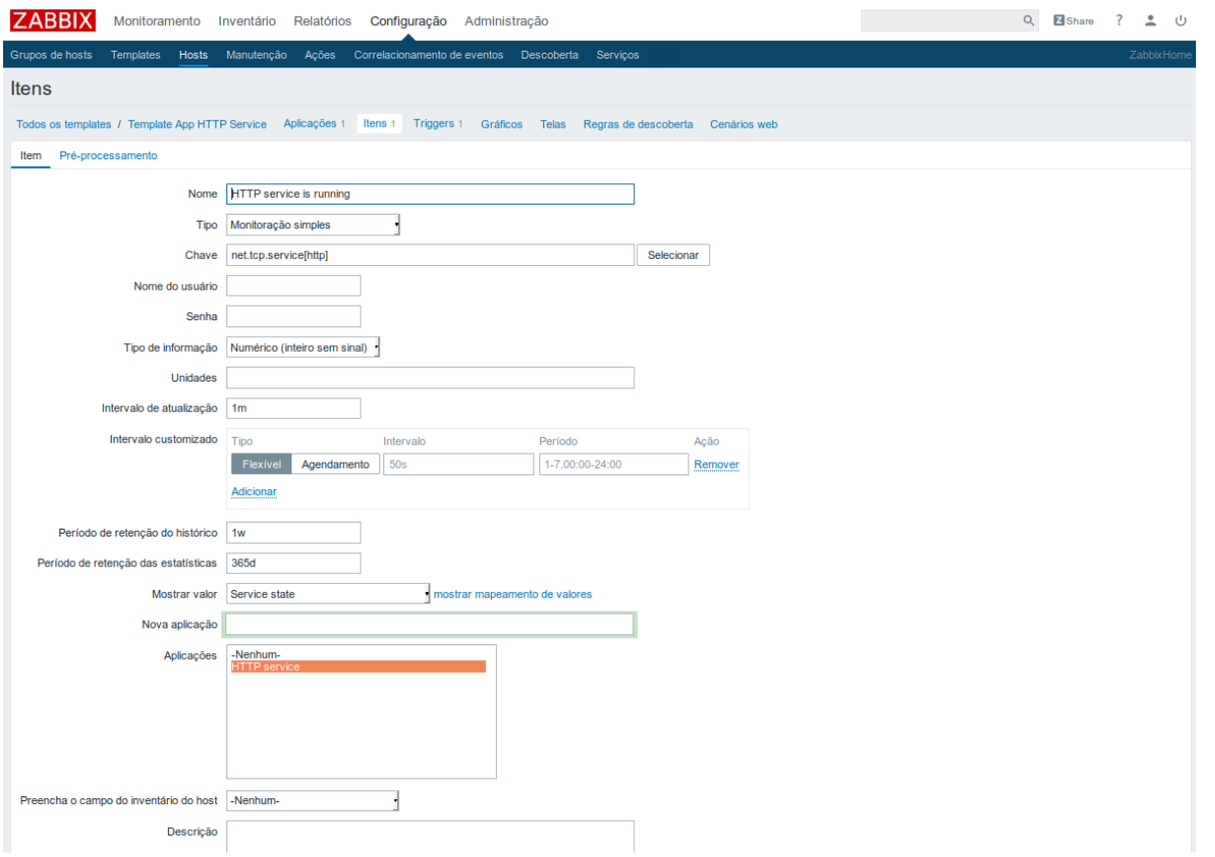


Figura 9: Exemplo de configuração de um item de monitoramento

Fonte: do autor.

Como ponto fraco destaco que é uma solução que possui uma curva de aprendizado grande para seu domínio completo em função da sua grande quantidade de recursos. O segundo ponto fraco, que considero o mais importante, é o fato de não haver uma categoria de templates pré-configurados com recursos mais sofisticados em relação à segurança da informação, embora seja possível a sua construção pelo administrador do Zabbix.

6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA

6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

A questão da segurança da informação é muito complexa e dinâmica. Somente através de ferramentas bem configuradas e atualizadas, pode-se reduzir de forma considerável seus riscos. Conforme o objetivo geral deste trabalho, que é identificar se o monitoramento de ativos e serviços de infraestrutura de rede, realizado com o Zabbix, pode contribuir com a segurança da informação das organizações, é importante destacar que o Zabbix possui muitos templates pré-configurados, focados na questão da disponibilidade dos ativos e serviços de TI, mas não na questão da segurança da informação, embora já possua recursos que poderiam contribuir muito mais com este tópico.

Para uma maior contribuição com a segurança da informação, seria muito útil se o Zabbix disponibilizasse uma categoria de templates pré-configurados, no processo de instalação do software, focados na segurança da informação, gerando alertas de eventos suspeitos que precisariam ser registrados e investigados pela equipe de segurança da informação das empresas.

Para a criação destes templates será necessário um levantamento dos itens relacionados com a segurança, por uma equipe de especialistas em segurança da informação, que em seguida deverão elaborar quais triggers devem ser implementadas de acordo com cada item de monitoramento relacionado. Após esta etapa, um analista de monitoramento deverá criar os templates oficiais que a serem incorporados em uma versão posterior do Zabbix.

6.2 RESULTADOS ESPERADOS

O que se espera com a disponibilização de templates pré-configurados voltados para a segurança da informação, é melhorar a inteligência da aplicação para detectar uma quantidade maior de eventos que podem se tornar uma ameaça e, portanto, precisam ser analisados e investigados pelas equipes responsáveis pela manutenção de rede das empresas. Eventos estes que podem passar despercebidos por uma equipe de segurança da informação se uma ferramenta adequada, com esta finalidade, não estiver sido implementada. Aplicações proprietárias com esta finalidade, geralmente possuem um custo de licenciamento muito elevado.

Para exemplificar como um template relacionado com a segurança da informação poderia reduzir os riscos nas empresas, ele poderia detectar a média de tráfego de um servidor de aplicação por horário, por dia da semana, por dia do mês, etc. Caso o volume de tráfego deste servidor sofra uma grande alteração em relação à sua média em um determinado perío-

do, seria gerado um alerta de segurança para ser analisado e para que sua causa seja investigada.

Fazendo uma análise e identificando, o quanto antes, as causas das variações anormais, aumenta-se consideravelmente a possibilidade de mitigação de riscos relacionados com segurança da informação e consequentemente as empresas poderão obter um retorno maior sobre o investimento realizado nos recursos de TI, podendo, em alguns casos, evitar um enorme prejuízo financeiro ou até mesmo a descontinuidade de suas atividades.

6.3 VIABILIDADE DA PROPOSTA

Como o Zabbix é uma aplicação de código fonte aberto e faz parte da cultura do desenvolvimento deste tipo de software receber contribuições de especialistas e de empresas que utilizam e investem em seu desenvolvimento, é possível fazer sugestões no fórum oficial da aplicação para o desenvolvimento destes templates pré-configurados.

Uma alternativa seria contratar a própria equipe de desenvolvimento do Zabbix para criar estes templates. No site do Zabbix encontramos uma tabela para contratação de serviços de desenvolvimento de templates a U$ 750,00/dia.

Tabela 2: Plano de mudanças

Etapa	Prazo em dias
Levantamento dos itens de monitoramento	5
Elaboração das triggers	2
Criação dos templates	1

Fonte: Do autor

Tabela 3: Recursos necessários

Recurso	Quantidade
Recursos humanos (Gerente de projetos)	1
Recursos financeiros	R$ 19.200,00
Recursos de TI (Especialistas em segurança e analista de desenvolvimento de templates)	2

Fonte: Do autor

7 CONSIDERAÇÕES FINAIS

Na realização deste trabalho, buscou-se desenvolver propostas para a melhoria dos recursos oferecidos pelo Zabbix com o objetivo de fornecer uma aplicação com mais ênfase na questão da segurança da informação, mitigando os riscos para as empresas que possuem uma infraestrutura de TI.

Acredita-se que fazendo uso das propostas apresentadas neste estudo, o software se tornará mais competitivo no mercado, apesar de ser um software com licença livre de custos, a empresa que o desenvolve possui receitas com serviços provenientes do seu produto.

Conforme demonstrou-se nos gráficos incluídos neste trabalho, verificou-se que todos os objetivos propostos foram alcançados. Constatou-se que o Zabbix é capaz de monitorar a disponibilidade de dispositivos e serviços de rede, gerar alertas de incidentes em caso de indisponibilidade e desta forma contribuir de forma significativa para a redução do downtime de serviços de rede, já que, a partir de um alerta gerado, o processo de tratamento de incidentes pode ser iniciado com maior agilidade nas empresas.

O grande desafio foi encontrar um tema a ser abordado que pudesse trazer uma proposta de melhoria e que pudesse ser bem aproveitado pelas empresas que necessitam aumentar o nível de segurança da informação. Após uma pesquisa na Internet em busca dos temas mais importantes, que estão recebendo atenção e investimentos das empresas, cheguei à conclusão do tema abordado neste trabalho.

Os obstáculos encontrados no desenvolvimento do projeto foram as poucas obras literárias disponíveis sobre o Zabbix, a criação do laboratório para a realização do estudo que envolveu a instalação e configuração de diversos softwares que permitissem o monitoramento da rede local. Sendo assim, foi necessário efetuar pesquisas na Internet e encontrei no próprio site oficial do Zabbix, informações importantes para a realização deste trabalho.

Deixo como sugestão para pesquisas futuras o levantamento de outros softwares de monitoramento de código aberto que também possam contribuir com a segurança da informação nas empresas.

REFERÊNCIAS

GONÇALVES, Marcus. **Firewalls Guia Completo**. Ciência Moderna, 2000.

HORST, Adail; PIRES Aécio e DÉO, André. **De A a ZABBIX**. Novatec, 2015.

UFRGS. Métodos de Pesquisa. Porto Alegre: UFRGS, 2009.

ZABBIX. Disponível em: <https://www.zabbix.com/presentation>. Acesso em: 10 set. 2017